paloalto NETWORKS

the network security company™

Palo Alto Networks®

Guía de implementación de VM-Series
PAN-OS 6.1

Información de contacto

Sede de la empresa:

Palo Alto Networks

4401 Great America Parkway

Santa Clara, CA 95054

http://www.paloaltonetworks.com/contact/contact/

Acerca de esta guía

Esta guía describe cómo configurar y obtener una licencia para el cortafuegos VM-Series, y está dirigida a administradores que deseen implementar el cortafuegos VM-Series.

Para obtener más información, consulte las siguientes fuentes:

- Guía del administrador de PAN-OS: para obtener instrucciones sobre cómo configurar las funciones del cortafuegos.
- https://paloaltonetworks.com/documentation: para acceder a bases de conocimientos, a un completo conjunto de documentación, foros de discusión y vídeos.
- https://support.paloaltonetworks.com: para ponerse en contacto con el equipo de asistencia técnica, obtener información sobre los programas de asistencia técnica o gestionar la cuenta o los dispositivos.
- Si desea las notas de versión más recientes, vaya a la página de descargas de software en https://support.paloaltonetworks.com/Updates/SoftwareUpdates.

Para enviar sus comentarios sobre la documentación, diríjase a: documentation@paloaltonetworks.com.

Palo Alto Networks, Inc.
www.paloaltonetworks.com
©2014, Palo Alto Networks, Inc. Todos los derechos reservados.
Palo Alto Networks y PAN-OS son marcas comerciales registradas de Palo Alto Networks, Inc.

Fecha de revisión: abril 24, 2015

Contenido

Acerca del cortafuegos VM-Series 1

Modelos de VM-Series 2

Implementaciones de VM-Series 3

Aplique la licencia y actualice el Cortafuegos VM-Series 5
- Creación de una cuenta de asistencia técnica 5
- Registro del cortafuegos VM-Series 6
- Activación de la licencia 7
- Actualización de la versión de software de PAN-OS (versión independiente) 9
- Actualización de la versión de software de PAN-OS (edición NSX) 10
- Actualización del modelo VM-Series 12

Configuración de un Cortafuegos VM-Series en un servidor ESXi 13

Implementaciones compatibles en el hipervisor vSphere de VMware (ESXi) 14

Requisitos y limitaciones del sistema 15
- Requisitos 15
- Limitaciones 16

Instale un Cortafuegos VM-Series en el hipervisor vSphere de VMware (ESXi) 17
- Aprovisionamiento del cortafuegos VM-Series en un servidor ESXi 17
- Configuración inicial en VM-Series en ESXi 20

Solución de problemas de implementaciones de ESXi 21
- Solución de problemas básicos 21
- Problemas de instalación 21
- Problemas de licencia 24
- Problemas de conectividad 24

Configuración de un Cortafuegos VM-Series en el servidor Citrix SDX 27

Acerca del cortafuegos VM-Series en el servidor SDX 28

Requisitos y limitaciones del sistema 29
- Requisitos 29
- Limitaciones 30

Implementaciones compatibles: Cortafuegos VM Series en Citrix SDX 31
- Situación 1: Protección del tráfico vertical 31
- Situación 2: Protección del tráfico horizontal (cortafuegos VM-Series en Citrix SDX) 34

Instalación del Cortafuegos VM-Series en el servidor SDX 35
- Carga de la imagen en el servidor SDX 35
- Aprovisionamiento del cortafuegos VM-Series en el servidor SDX 36

Tráfico vertical seguro con el cortafuegos VM-Series 37
- Implementación del cortafuegos VM-Series con interfaces de capa 3 37
- Implementación del cortafuegos VM-Series con interfaces de capa 2 (L2) o de cable virtual 41
- Implementación del cortafuegos VM-Series antes de la NetScaler VPX 44

Tráfico horizontal con el cortafuegos VM-Series 47

Configuración del cortafuegos VM-Series edición NSX 49

Presentación del cortafuegos VM-Series edición NSX 50
¿Cuáles son los componentes de la solución de la edición NSX? 51
¿Cómo se coordinan los componentes de la solución de la edición NSX? 55
¿Cuáles son las ventajas de la solución de la edición NSX? 61
Lista de comprobación de implementación del cortafuegos VM-Series edición NSX 62
Creación de un grupo de dispositivos y plantillas en Panorama 64
Registro del cortafuegos VM-Series como servicio en NSX Manager 65
Implementación del cortafuegos VM-Series 68
Habilite SpoofGuard 69
Definición de un grupo de direcciones IP 71
Preparación del host ESXi para el cortafuegos de VM-Series 72
Implementación del servicio Palo Alto Networks NGFW 73
Creación de políticas 76
Definición de políticas en el administrador NSX 77
Aplicación de políticas al cortafuegos de VM-Series 80
Envío del tráfico desde los invitados que no ejecutan VMware Tools 84
Grupos de direcciones dinámicas: Retransmisión de información desde NSX Manager a Panorama 85

Configuración del cortafuegos VM-Series en AWS 91

Acerca del cortafuegos VM-Series en AWS 92
Implementaciones compatibles con AWS 95
Implementación del cortafuegos VM-Series en AWS 97
Obtención de la AMI 97
Consulte los requisitos y limitaciones del sistema para VM-Series en AWS 97
Hoja de trabajo para la planificación de VM-Series en la VPC de AWS 98
Inicio del cortafuegos VM-Series en AWS 99
Caso de uso: Protección de las instancias de EC2 en AWS Cloud 106
Caso de uso: Uso de grupos de direcciones dinámicas para proteger las nuevas instancias de EC2 en la VPC 119
Lista de atributos supervisados en la VPC de AWS 123
Caso de uso: Cortafuegos VM-Series como puertas de enlace de GlobalProtect en AWS 124
Componentes de la infraestructura de GlobalProtect 125
Implementación de puertas de enlace de GlobalProtect en AWS 125

Configuración del cortafuegos VM-Series en KVM 127

VM-Series en KVM: Especificaciones y requisitos previos 128
Requisitos del sistema 128
Opciones para adjuntar el VM-Series en la red 129
Requisitos previos para VM-Series en KVM 129

Implementaciones compatibles con KVM 132
Protección del tráfico en un host único 132
Protección del tráfico a través de hosts Linux 133
Instalación del cortafuegos VM-Series en KVM 135
Habilitación del uso de un controlador SCSI 141
Comprobación de PCI-ID para la ordenación de interfaces de red en el cortafuegos VM-Series . . . 142
Uso de un archivo ISO para implementar el cortafuegos VM-Series 143

Acerca del cortafuegos VM-Series

El Cortafuegos VM-Series de Palo Alto Networks es la versión virtualizada de cortafuegos de última generación de Palo Alto Networks. Es ideal para su uso en un entorno virtualizado o en la nube, donde puede proteger tanto el tráfico horizontal como vertical.

- Modelos de VM-Series
- Implementaciones de VM-Series
- Aplique la licencia y actualice el Cortafuegos VM-Series

Modelos de VM-Series

El cortafuegos VM-Series está disponible en cuatro modelos (VM-100, VM-200, VM-300 y VM-1000-HV).

Los cuatro modelos pueden implementarse como máquinas virtuales invitadas en ESXi de VMware y NetScaler SDX de Citrix; en NSX de VMWare sólo se admite VM-1000-HV. El paquete de software (archivo *.xva* o *.ovf*) que se usa para implementar el cortafuegos VM-Series es común en todos los modelos. El modelo VM-Series funciona con licencia; cuando aplica la licencia en el cortafuegos VM-Series, el número de modelo y las capacidades asociadas se implementan en el cortafuegos.

Cada modelo puede adquirirse en versión Individual o Enterprise. La versión Individual se vende por unidades. El SKU que solicite, por ejemplo PA-VM-300, incluye un código de autenticación para obtener licencia de una instancia del cortafuegos VM-Series. La versión Enterprise está disponible en bloques de 25 unidades. Por ejemplo, el SKU de pedido PAN-VM-100-ENT tiene un único código de autenticación que le permite registrar 25 instancias del VM-100.

Cada modelo de cortafuegos VM-Series tiene licencia para una capacidad máxima. La capacidad se define por el número de sesiones, reglas, zonas de seguridad, objetos de dirección, túneles VPN de IPSec y túneles VPN de SSL que el cortafuegos VM-Series está optimizado para gestionar. Al adquirir una licencia, asegúrese de que adquiere la licencia correcta basándose en sus requisitos de red. La siguiente tabla describe algunas de las diferencias de capacidad por modelo:

Modelo	Sesiones	Reglas de seguridad	Direcciones IP dinámicas	Zonas de seguridad	Túneles VPN de IPSec	Túneles VPN de SSL
VM-100	50000	250	1000	10	25	25
VM-200	100000	2000	1000	20	500	200
VM-300	250000	5000	1000	40	2000	500
VM-1000-HV	250000	10000	100000	40	2000	500

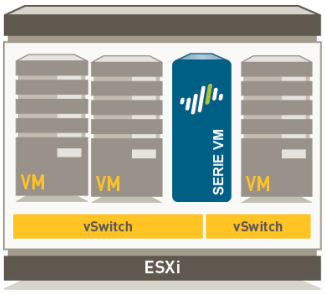
Para obtener información sobre las plataformas en las que puede implementar el cortafuegos VM-Series, consulte Implementaciones de VM-Series. Para obtener información general, consulte Acerca del cortafuegos VM-Series.

Implementaciones de VM-Series

El cortafuegos VM-Series puede implementarse en las siguientes plataformas:

VM-Series para el hipervisor vSphere de VMware (ESXi)

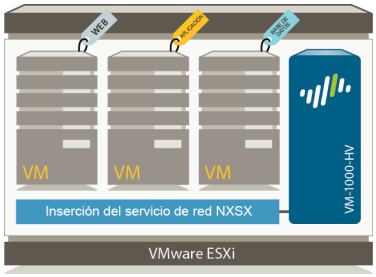
VM-100, VM-200, VM-300 o VM-1000-HV se implementan como máquina virtual invitada en ESXi de VMware; ideal para redes o nubes en las que es necesaria una versión virtual.



Para obtener más información, consulte Configuración de un Cortafuegos VM-Series en un servidor ESXi.

VM-Series para NSX de VMware

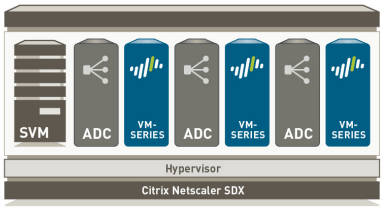
El modelo VM-1000-HV se implementa como un servicio de introspección de red con NSX de VMware y Panorama. La implementación es ideal para la inspección de tráfico horizontal, y también puede proteger el tráfico vertical.



Si desea información detallada, consulte Configuración del cortafuegos VM-Series edición NSX

VM-Series para SDX de Citrix

VM-100, VM-200, VM-300 o VM-1000-HV se implementan como máquina virtual invitada en NetScaler SDX de Citrix; consolida los servicios de seguridad y ADC y las implementaciones de XenApp/XenDesktop de Citrix.



Si desea información detallada, consulte Configuración de un Cortafuegos VM-Series en el servidor Citrix SDX

- **VM-Series para Amazon Web Services (AWS)**

  VM-100, VM-200, VM-300 o VM-1000-HV se pueden implementar en instancias EC2 en AWS Cloud.

  Para obtener más información, consulte Configuración del cortafuegos VM-Series en AWS.

- **VM-Series para módulo de virtualización de Kernel (KVM)**

  VM-100, VM-200, VM-300 o VM-1000-HV se pueden implementar en un servidor Linux que ejecute el hipervisor KVM. Para obtener más información, consulte Configuración del cortafuegos VM-Series en KVM.

A continuación, se incluye una breve descripción de los requisitos para implementar el cortafuegos VM-Series:

Implementación	Versiones de hipervisor compatibles	Imagen base necesaria en el portal de asistencia técnica de Palo Alto Networks	Licencias de capacidad correspondientes
VM-Series para el hipervisor vSphere de VMware (ESXi) (sin NSX de VMware)	5.0, 5.1 y 5.5	**PAN-OS para imágenes base de VM-Series** Por ejemplo, el nombre de la imagen descargable es: **PA-VM-6.1.0.zip**	VM-100 VM-200 VM-300 VM-1000-HV
VM-Series para NSX de VMware vSphere con NSX de VMware y Panorama	5.5	**PAN-OS para imágenes base NSX de VM-Series** Por ejemplo, el nombre de la imagen descargable es: **PA-VM-NSX-6.0.0.zip**	VM-1000-HV
VM-Series para SDX de Citrix Versión de SDX Versión de XenServer	10.1+ 6.0.2 o superior	**PAN-OS imágenes base de SDX de VM-Series** Por ejemplo, el nombre de la imagen descargable es: **PA-VM-SDX-6.1.0.zip**	VM-100 VM-200 VM-300 VM-1000-HV
VM-Series para AWS	N/D	**N/D**	VM-100 VM-200 VM-300 VM-1000-HV
VM-Series para KVM	KVM en las siguientes distribuciones de Linux: • Ubuntu: 12.04 LTS • CentOS/ RedHat Enterprise Linux: 6.5	**PAN-OS para imágenes base KVM de VM-Series** Por ejemplo, el nombre de la imagen descargable es: **PA-VM-6.1.0.qcow2**	VM-100 VM-200 VM-300 VM-1000-HV

Aplique la licencia y actualice el Cortafuegos VM-Series

Cuando adquiere un cortafuegos VM-Series recibe un conjunto de códigos de autenticación por correo electrónico. El correo electrónico suele incluir códigos de autorización para aplicar la licencia al modelo de VM-Series adquirido (VM-100, VM-200, VM300, VM-1000-HV), el derecho de asistencia que le permite acceder a las actualizaciones de contenido y software (por ejemplo, PAN-SVC-PREM-VM-100 SKU auth-code), y cualquier suscripción adicional como prevención de amenazas, filtrado URL, GlobalProtect o WildFire. En el caso de la solución NSX integrada en VMware, el correo electrónico contiene un único código de autorización que agrupa la licencia de capacidad para una o más instancias del modelo VM-1000-HV, el derecho de asistencia y una o más licencias de suscripción.

Para usar los códigos de autorización, debe registrar el código en la cuenta de asistencia del portal de asistencia de Palo Alto Network. Si ya tiene una cuenta de asistencia técnica, puede acceder al enlace **Código de autenticación de VM-Series** de la página de software de asistencia técnica para gestionar sus licencias del Cortafuegos VM-Series y descargar el software.

Si aún no dispone de una cuenta de asistencia técnica, deberá facilitar su número de pedido de venta o ID de cliente y el código de autenticación de capacidad para registrar y crear una cuenta en el portal de asistencia. Una vez se verifique su cuenta y finalice el registro, podrá iniciar sesión y descargar el paquete de software necesario para instalar el Cortafuegos VM-Series. Para obtener información sobre la activación de la licencia para su implementación, consulte la sección correspondiente en Activación de la licencia.

Si tiene una copia de evaluación del cortafuegos VM-Series y desea convertirlo en una copia con licencia completa (adquirida), clone su cortafuegos VM-Series y use las instrucciones para registrar y asignar una licencia a la copia adquirida de su cortafuegos VM-Series. Para obtener instrucciones, consulte Actualización del modelo VM-Series.

Para adquirir una licencia para su cortafuegos VM-Series, consulte las siguientes secciones:

- Creación de una cuenta de asistencia técnica
- Registro del cortafuegos VM-Series
- Activación de la licencia
- Actualización de la versión de software de PAN-OS (versión independiente)
- Actualización de la versión de software de PAN-OS (edición NSX)
- Actualización del modelo VM-Series

Si desea instrucciones sobre la instalación de su cortafuegos VM-Series, consulte Implementaciones de VM-Series.

Creación de una cuenta de asistencia técnica

Se necesita una cuenta de asistencia técnica para gestionar sus licencias del Cortafuegos VM-Series y descargar el paquete de software necesario para instalar el cortafuegos VM-Series. Si ya tiene una cuenta de asistencia técnica, continúe con Registro del cortafuegos VM-Series.

Creación de una cuenta de asistencia técnica

1. Inicie sesión en https://support.paloaltonetworks.com/.
2. Haga clic en **Registrar** y cumplimente los detalles en el formulario de registro de usuarios. Debe usar el código de autenticación de capacidad y el número de pedido de compra o venta para registrar y crear una cuenta en el portal de asistencia técnica.
3. **Envíe** el formulario. Recibirá un correo electrónico con un vínculo para activar la cuenta de usuario; complete los pasos para activar la cuenta.

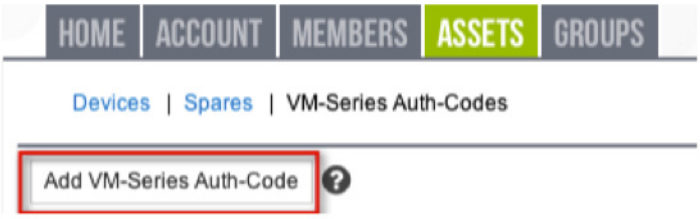
   Una vez se verifique su cuenta y finalice el registro, podrá iniciar sesión y descargar el paquete de software necesario para instalar el Cortafuegos VM-Series.

Registro del cortafuegos VM-Series

Siga las instrucciones de esta sección para registrar su código de autenticación de capacidad con su cuenta de asistencia técnica.

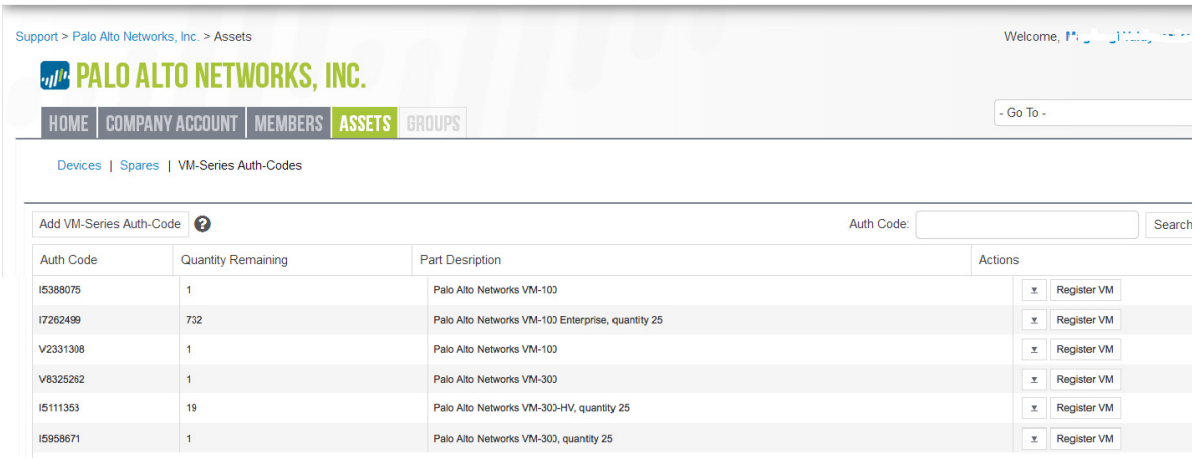
Registro del cortafuegos VM-Series

1. Inicie sesión en https://support.paloaltonetworks.com con sus credenciales de cuenta.
2. Seleccione **Activos** y haga clic en **Añadir códigos de autenticación de VM-Series.**



3. En el campo **Añadir códigos de autenticación de VM-Series**, introduzca el código de autenticación de capacidad que recibió por correo electrónico y haga clic en la marca de verificación a la derecha para guardarlo. La página mostrará la lista de códigos de autenticación registrados en su cuenta de asistencia técnica.

   Puede hacer un seguimiento del número de cortafuegos VM-Series que se han implementado y el número de licencias que siguen disponibles con cada código de autenticación. Cuando se hayan usado todas las licencias disponibles, el código de autenticación dejará de aparecer en la página Códigos de autenticación de VM-Series. Para ver todos los activos que se han implementado, seleccione **Activos > Dispositivos**.



Activación de la licencia

Para activar la licencia en su cortafuegos VM-Series, deberá haber implementado el cortafuegos VM-Series y haber completado la configuración inicial. Si desea instrucciones sobre la implementación del cortafuegos VM-Series, consulte Implementaciones de VM-Series.

Hasta que haya activado la licencia en el cortafuegos VM-Series, el cortafuegos no tendrá un número de serie, la dirección MAC de las interfaces del plano de datos no serán únicas y sólo se admitirá un número mínimo de sesiones. Como las direcciones MAC no son únicas hasta que el cortafuegos recibe licencia, para evitar problemas por superposición de direcciones MAC asegúrese de no tener múltiples cortafuegos VM-Series sin licencia.

Cuando activa la licencia, el servidor de licencias usa la UUID y la Id. de la CPU de la máquina virtual para generar un número de serie único para el cortafuegos VM-Series. El código de autenticación de capacidad, junto con el número de serie, se usa para validar su autorización.

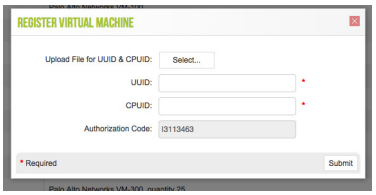
Tras aplicar la licencia a un cortafuegos VM-Series, si elimina y vuelve a implementar el cortafuegos VM-Series en el mismo host (algo habitual sólo en un entorno de laboratorio), use un nombre exclusivo cuando vuelva a implementar el cortafuegos. El uso de un nombre exclusivo garantiza que el UUID asignado al cortafuegos no es el mismo que el asignado a la instancia eliminada del cortafuegos. El UUID exclusivo es obligatorio para completar el proceso de licencia sin problemas.

- Activación de la licencia para el cortafuegos VM-Series (versión independiente)
- Activación de la licencia para el cortafuegos VM-Series edición NSX

Activación de la licencia para el cortafuegos VM-Series (versión independiente)

Para activar la licencia en su cortafuegos VM-Series, deberá haber implementado el cortafuegos VM-Series y haber completado la configuración inicial.

Activación de la licencia	
• Si su cortafuegos VM-Series no tiene acceso directo a Internet. Para activar la licencia, el cortafuegos debe estar configurado con una dirección IP, máscara de red, puerta de enlace predeterminada y dirección IP de servidor DNS.	1. Seleccione **Dispositivo > Licencias** y seleccione el vínculo **Activar función usando el código de autenticación**. 2. Introduzca el código de autenticación de capacidad que registró en el portal de asistencia técnica. El cortafuegos se conectará con el servidor de actualización (updates.paloaltonetworks.com), descargará la licencia y se reiniciará automáticamente. 3. Vuelva a iniciar sesión en la interfaz web y confirme que el **Panel** muestra un número de serie válido. Si aparece el término *Desconocido*, significa que el dispositivo no tiene licencia. 4. En **Dispositivo > Licencias**, compruebe que se añade la licencia **PA-VM** al dispositivo.

Activación de la licencia (Continuación)	
• Si su cortafuegos VM-Series tiene acceso directo a Internet	1. Seleccione **Dispositivo > Licencias** y haga clic en el vínculo **Activar función usando el código de autenticación**. 2. Haga clic en **Descargar archivo de autorización** y descargue *authorizationfile.txt* en la máquina cliente. 3. Copie *authorizationfile.txt* en un ordenador que tenga acceso a Internet e inicie sesión en el portal de asistencia técnica. Haga clic en el vínculo **Mis códigos de autenticación de VM-Series** y seleccione el código de autenticación aplicable en la lista y haga clic en el vínculo **Registrar VM**. 4. Cargue el archivo de autorización en la ficha **Registrar máquina virtual**. Esto completará el proceso de registro y el número de serie y el cortafuegos VM-Series se añadirá a sus registros de cuenta.  5. Desplácese hasta **Activos > Mis dispositivos**, busque el dispositivo VM-Series que acaba de registrar y haga clic en el vínculo **PA-VM**. Esto descargará la clave de licencia de VM-Series en la máquina cliente. 6. Copie la clave de licencia en la máquina que puede acceder a la interfaz web del cortafuegos VM-Series y desplácese hasta **Dispositivo > Licencias**. 7. Haga clic en **Clave de licencia de carga manual** e introduzca la clave de licencia. Cuando la licencia de capacidad se haya activado en el cortafuegos se producirá el reinicio. 8. Inicie sesión en el dispositivo y confirme que el **Panel** muestra un número de serie válido y que la licencia muestra **PA-VM** en la ficha **Dispositivo > Licencias**.

Activación de la licencia para el cortafuegos VM-Series edición NSX

Panorama sirve como punto central de administración de los cortafuegos VM-Series de la edición NSX y el proceso de activación de licencia es automático. Cuando se implementa un nuevo cortafuegos VM-Series edición NSX, se comunica con Panorama para obtener la licencia. Por lo tanto, necesita asegurarse de que Panorama tiene acceso a Internet y puede conectar con el servidor de actualizaciones de Palo Alto Networks para recuperar las licencias. Para obtener una descripción general de los componentes y requisitos de implementación del cortafuegos VM-Series edición NSX, consulte Presentación del cortafuegos VM-Series edición NSX.

Para esta solución integrada, el código de autenticación (por ejemplo, PAN-VM-!000-HV-SUB-BND-NSX2) incluye licencias para la prevención de amenazas, filtrado de URL, suscripciones a WildFire y asistencia premium para el período requerido.

Para activar la licencia, debe haber completado las siguientes tareas:

- Registrar el código de autenticación en la cuenta de asistencia. Si no registra el código de autenticación, el servidor de licencias no podrá crear una licencia.
- Configurar el administrador de servicios VMware e introducir este código de autenticación en Panorama. En Panorama, seleccione **Administrador de servicios VMWare** para añadir el **código de autorización**.

Si ha adquirido un código de autenticación de prueba, puede activar la licencia hasta en un máximo de 5 cortafuegos VM-Series con licencias de capacidad VM-1000-HV durante un período de 30 o 60 días. Dado que esta solución le permite implementar un cortafuegos VM-Series por host ESXi, el clúster de ESXi puede incluir un máximo de 5 hosts ESXi si se usa una licencia de prueba.

Para activar la licencia, debe completar las siguientes tareas:

- Compruebe que los cortafuegos VM-Series que acaba de implementar se muestran como **Dispositivos gestionados** y están conectados a Panorama.
- Seleccione **Panorama > Implementación de dispositivo > Licencias** y haga clic en **Actualizar**. Seleccione los cortafuegos VM-Series para los que quiere recuperar licencias de suscripción y haga clic en **ACEPTAR**.

  Panorama aplicará las licencias a cada cortafuegos que se haya implementado con el código de autenticación coincidente.

Actualización de la versión de software de PAN-OS (versión independiente)

Ahora que el Cortafuegos VM-Series tiene conectividad de red y el software PAN-OS básico está instalado, debería actualizarlo a la versión más reciente de PAN-OS. Use las siguientes instrucciones para cortafuegos que no están implementados en una configuración de alta disponibilidad (HA). Para cortafuegos implementados en HA, consulte la Guía de nuevas funciones de PAN-OS 6.1.

Actualización de la versión de PAN-OS (versión independiente)

1. Desde la interfaz web, desplácese hasta **Dispositivo > Licencias** y asegúrese de que tiene la licencia correcta para el Cortafuegos VM-Series y que la licencia está activada.

   En la versión independiente del cortafuegos VM-Series, vaya a **Dispositivo > Asistencia técnica** y asegúrese de que tiene activada la licencia de asistencia técnica.
2. (Necesario para un cortafuegos en uso) Guarde una copia de seguridad del archivo de configuración actual.
   a. Seleccione **Dispositivo > Configuración > Operaciones** y haga clic en **Exportar instantáneas de configuración con nombre**.
   b. Seleccione el archivo XML que contiene su configuración en uso (por ejemplo, **running-config.xml**) y haga clic en **ACEPTAR** para exportar el archivo de configuración.
   c. Guarde el archivo exportado en una ubicación externa al cortafuegos. Puede usar esta copia de seguridad para restaurar la configuración si tiene problemas con la actualización.

Actualización de la versión de PAN-OS (versión independiente) (Continuación)

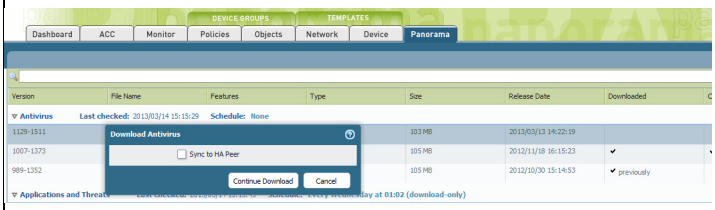
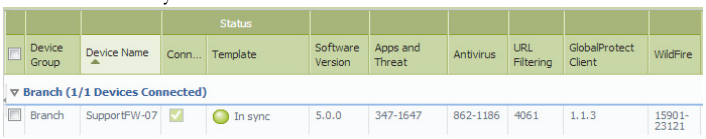
3. Consulte las notas de la versión para comprobar la versión de la publicación de contenido necesaria para la versión de PAN-OS. Los cortafuegos que vaya a actualizar deberán estar ejecutando la versión de publicación de contenido necesaria para la versión de PAN-OS.
   a. Seleccione **Dispositivo > Actualizaciones dinámicas**.
   b. Consulte la sección **Aplicaciones y amenazas** o **Aplicaciones** para saber qué actualización está en ejecución actualmente.
   c. Si el cortafuegos no está ejecutando la actualización requerida o posterior, haga clic en **Comprobar ahora** para recuperar una lista de actualizaciones disponibles.
   d. Busque la actualización que prefiera y haga clic en **Descargar**.
   e. Cuando finalice la descarga, haga clic en **Instalar**.
4. Actualice la versión de PAN-OS en el Cortafuegos VM-Series.
   a. Seleccione **Dispositivo > Software**.
   b. Haga clic en **Actualizar** para ver la versión de software más reciente; asimismo, revise **Notas de versión** para ver una descripción de los cambios de una versión y la ruta de migración para instalar el software.
   c. Haga clic en **Descargar** para recuperar el software y, a continuación, haga clic en **Instalar**.

Actualización de la versión de software de PAN-OS (edición NSX)

Para el cortafuegos VM-Series edición NSX, use Panorama para actualizar la versión de software en los cortafuegos.

Actualización de los cortafuegos VM-Series edición NSX mediante Panorama

Paso 1	Guarde una copia de seguridad del archivo de configuración actual en cada cortafuegos gestionado que quiera actualizar. Aunque el cortafuegos creará automáticamente una copia de seguridad de la configuración, se recomienda crear una copia de seguridad antes de actualizar y almacenarla externamente.	1. Seleccione **Dispositivo > Configuración > Operaciones** y haga clic en **Exportar Panorama y lote de configuración de dispositivos**. Esta opción se utiliza para generar manualmente y exportar la versión más reciente de la copia de seguridad de configuración de Panorama y de los dispositivos gestionados. 2. Guarde el archivo exportado en una ubicación externa al cortafuegos. Puede usar esta copia de seguridad para restaurar la configuración si tiene problemas con la actualización.

Actualización de los cortafuegos VM-Series edición NSX mediante Panorama (Continuación)		
Paso 2	Consulte las notas de la versión para comprobar la versión de la publicación de contenido necesaria para la versión de PAN-OS. Los cortafuegos que vaya a actualizar deberán estar ejecutando la versión de publicación de contenido necesaria para la versión de PAN-OS.	1. Seleccione **Panorama > Device Deployment (Implementación de dispositivos) > Actualizaciones dinámicas**. 2. Compruebe las actualizaciones más recientes. Haga clic en **Comprobar ahora** (ubicado en la esquina inferior izquierda de la ventana) para comprobar las actualizaciones más recientes. El enlace de la columna **Acción** indica si una actualización está disponible. Si una versión está disponible, se muestra el enlace **Descargar**.  3. Haga clic en **Descargar** para descargar una versión seleccionada. Tras una descarga correcta, el enlace de la columna **Acción** cambia de **Descargar** a **Instalar**. 4. Haga clic en **Instalar** y seleccione los dispositivos en los que desee instalar la actualización. Cuando se complete la instalación, aparecerá una marca de verificación en la columna **Instalado actualmente**.
Paso 3	Implemente las actualizaciones de software en los cortafuegos seleccionados. Si tiene dispositivos configurados en HA, asegúrese de borrar la casilla de verificación **Agrupar peers de HA** y actualice cada peer de HA por separado.	1. Seleccione **Panorama > Device Deployment (Implementación de dispositivos) > Software**. 2. Compruebe las actualizaciones más recientes. Haga clic en **Comprobar ahora** (ubicado en la esquina inferior izquierda de la ventana) para comprobar las actualizaciones más recientes. El enlace de la columna **Acción** indica si una actualización está disponible. 3. Revise el **Nombre de archivo** y haga clic en **Descargar**. Verifique que las versiones de software que ha descargado coinciden con los modelos de cortafuegos implementados en su red. Tras una descarga correcta, el enlace de la columna **Acción** cambia de **Descargar** a **Instalar**. 4. Haga clic en **Instalar** y seleccione los dispositivos en los que desee instalar la versión de software. 5. Seleccione **Reiniciar dispositivo tras instalar** y haga clic en **ACEPTAR**. 6. Si tiene dispositivos configurados en HA, borre la casilla de verificación **Agrupar peers de HA** y actualice cada peer de HA por separado.
Paso 4	Verifique la versión de actualización de contenido y de software que se ejecutan en cada dispositivo gestionado.	1. Seleccione **Panorama > Dispositivos gestionados**. 2. Ubique los dispositivos y revise el contenido y las versiones de contenido y de software en la tabla. 

Actualización del modelo VM-Series

El proceso de licencia del cortafuegos de la serie usa la UUID y la Id. de CPU para generar un número de serie único para cada cortafuegos VM-Series. Así, cuando genera una licencia, esta se asigna a una instancia específica del cortafuegos VM-Series y no puede modificarse.

Para aplicar una nueva licencia de capacidad a un cortafuegos que ya tuviera una licencia, deberá duplicar el cortafuegos VM-Series existente (totalmente configurado). Durante el proceso de duplicación, el cortafuegos se asigna a un UUID exclusivo y, por lo tanto, puede aplicar una nueva licencia a la instancia duplicada del cortafuegos.

Use las instrucciones de la sección si está:

- Migrando desde una licencia de evaluación a otra de producción.
- Actualizando el modelo para permitir una mayor capacidad. Por ejemplo, si desea actualizar del VM-200 a la licencia de VM-1000-HV.

Migración de la licencia del cortafuegos VM-Series		
Paso 1	Desactive el cortafuegos VM-Series.	
Paso 2	Clone el cortafuegos VM-Series.	Si está clonando de forma manual, cuando se le pregunte indique que está copiando el cortafuegos, no moviéndolo.
Paso 3	Encienda la nueva instancia del cortafuegos VM-Series.	1. Inicie la consola de número de serie del cortafuegos en la interfaz web de vSphere/SDX e introduzca el siguiente comando: `show system info` 2. Compruebe que: • el número de serie es desconocido • el cortafuegos no tiene licencias • la configuración está intacta
Paso 4	Registre el nuevo código de autenticación en el portal de asistencia.	Consulte Registro del cortafuegos VM-Series.
Paso 5	Aplique la nueva licencia	Consulte Activación de la licencia. Tras aplicar correctamente la licencia al nuevo cortafuegos, elimine la instancia anterior del cortafuegos para evitar conflictos en la configuración o las asignaciones de direcciones IP.

Configuración de un Cortafuegos VM-Series en un servidor ESXi

El Cortafuegos VM-Series se distribuye mediante el formato abierto de virtualización (OVF), que es un método estándar de empaquetar e implementar máquinas virtuales. Puede instalar esta solución en cualquier dispositivo x86 capaz de ejecutar VMware ESXi.

Para implementar un cortafuegos VM-Series debe estar familiarizado con VMware y vSphere, incluidas las redes vSphere, la instalación y configuración de host ESXi y la implementación de máquinas virtuales invitadas.

Si desea automatizar el proceso de implementación de un cortafuegos VM-Series, puede crear una plantilla estándar de referencia con la configuración y políticas óptimas y usar la API de vSphere y la API XML de PAN-OS para implementar rápidamente nuevos cortafuegos VM-Series en su red. Para obtener detalles, consulte el artículo: Automatización del centro de datos de VM-Series.

Consulte los siguientes temas si desea información sobre:

- Implementaciones compatibles en el hipervisor vSphere de VMware (ESXi)
- Requisitos y limitaciones del sistema
- Instale un Cortafuegos VM-Series en el hipervisor vSphere de VMware (ESXi)
- Solución de problemas de implementaciones de ESXi

Implementaciones compatibles en el hipervisor vSphere de VMware (ESXi)

Puede implementar una o varias instancias del cortafuegos VM-Series en el servidor ESXi. La ubicación del cortafuegos VM-Series en la red dependerá de su topología. Seleccione de las siguientes opciones (para entornos que no usan VMware NSX):

- **Un cortafuegos VM-Series por host ESXi**: todos los servidores VM del host ESXi atraviesan el cortafuegos antes de salir del host por la red física. Los servidores VM se adjuntan al cortafuegos a través de los conmutadores estándar virtuales. Los servidores invitados no tienen ninguna otra conectividad de red, por lo que el cortafuegos visualiza y controla todo el tráfico que sale del host ESXi. Una variación de este caso de uso es también exigir que todo el tráfico fluya por el cortafuegos, incluyendo el tráfico de servidor a servidor (tráfico horizontal) en el mismo host ESXi.
- **Un cortafuegos VM-Series por red virtual**: implemente un cortafuegos VM-Series para cada red virtual. Si ha diseñado su red de modo que uno o más hosts ESXi tengan un grupo de máquinas virtuales que pertenezcan a la red interna, un grupo que pertenezca a la red externa y otros a la DMZ; puede implementar un cortafuegos de la serie XM para salvaguardar los servidores de cada grupo. Si un grupo o red virtual no comparte un conmutador virtual o grupo de puertos con otra red virtual, estará totalmente aislado de las demás redes virtuales del host. Como no hay otra ruta física o virtual a ninguna otra red, los servidores de cada red virtual deben usar el cortafuegos para comunicarse con cualquier otra red. Esto ofrece al cortafuegos visibilidad y control sobre todo el tráfico que abandona el conmutador virtual (estándar o distribuido) adjunto a cada red virtual.
- **Entorno híbrido**: se usan tanto host físicos como virtuales, el cortafuegos VM-Series puede implementarse en una ubicación de agregación tradicional en lugar de un dispositivo de cortafuegos físico para conseguir los beneficios de una plataforma de servidor común para todos los dispositivos y para desvincular las dependencias de actualización de hardware y software.

Continúe con Requisitos y limitaciones del sistema e Instale un Cortafuegos VM-Series en el hipervisor vSphere de VMware (ESXi).

Requisitos y limitaciones del sistema

Esta sección enumera los requisitos y las limitaciones del cortafuegos VM-Series en el hipervisor vSphere de VMware (ESXi). Para implementar el cortafuegos VM-Series, consulte Instale un Cortafuegos VM-Series en el hipervisor vSphere de VMware (ESXi).

▲ Requisitos

▲ Limitaciones

Requisitos

Puede crear e implementar una o varias instancias del cortafuegos VM-Series en el servidor ESXi. Como todas las instancias del cortafuegos necesitan una asignación de recursos mínima (cantidad de CPU, memoria y espacio en disco) en el servidor ESXi, asegúrese de cumplir las especificaciones que aparecen a continuación para garantizar un rendimiento óptimo.

El Cortafuegos VM-Series tiene los siguientes requisitos:

- VMware ESXi con vSphere 5.0, 5.1 y 5.5 para VM-Series que ejecute PAN-OS 6.1.
- Un mínimo de dos vCPU por cada Cortafuegos VM-Series. una para el plano de gestión y la otra para el plano de datos.

  Puede asignar 2 o 6 vCPU adicionales para asignar un total de 2, 4 u 8 vCPU al cortafuegos; el plano de gestión sólo usa una vCPU y puede asignar las vCPU adicionales al plano de datos.
- Un mínimo de dos interfaces de red (vmNIC). Una será una vmNIC específica para la interfaz de gestión y la otra para la interfaz de datos. A continuación, podrá añadir hasta ocho vmNIC más para el tráfico de datos. Para añadir interfaces adicionales, use VLAN Guest Tagging (VGT) en el servidor ESXi o configure subinterfaces en el cortafuegos.

  Si está implementando el cortafuegos VM-Series mediante capa 2, cable virtual o interfaces tap, debe habilitar el modo promiscuo en el grupo de puertos del conmutador virtual al que se adjuntan las interfaces de datos en el cortafuegos. Si no está habilitado el modo promiscuo, el cortafuegos no recibirá tráfico porque las direcciones MAC de destino asignadas por PAN-OS serán diferentes de las direcciones MAC de vmNIC asignadas por vSphere. De manera predeterminada, vSphere no reenviará una trama a una máquina virtual si la dirección MAC de destino de la trama no coincide con la dirección MAC de vmNIC.

  Si está implementando el cortafuegos VM-Series usando interfaces de capa 3, en su lugar puede establecer direcciones MAC de vmNIC para que coincidan con las direcciones MAC de PAN-OS modificando manualmente la dirección MAC de cada vmNIC en vSphere para que coincida con lo asignado en el cortafuegos VM-Series. Este cambio debe realizarse mientras VM-Series está desactivado; permite que el cortafuegos reciba tramas que le corresponden.
- Un mínimo de 4 GB de memoria para todos los modelos excepto el VM-1000-HV, que necesita 5 GB. Cualquier memoria adicional se utilizará únicamente en el plano de gestión. Si está aplicando la licencia VM-1000-HV, consulte ¿Cómo puedo modificar el archivo de imagen base de la licencia de VM-1000-HV?
- Un mínimo de 40 GB de espacio de disco virtual. Puede añadir un disco adicional de 40 GB hasta 2 TB para almacenamiento de registros.

Limitaciones

Las prestaciones del Cortafuegos VM-Series son muy parecidas a las de los cortafuegos de hardware de Palo Alto Networks, pero con las siguientes limitaciones:

- Se recomienda usar núcleos CPU dedicados.
- Únicamente se admite la versión lite de alta disponibilidad (HA) (activo/pasivo sin conmutación por error con estado).
- La supervisión de enlaces de alta disponibilidad (HA) únicamente se admite en instalaciones de VMware ESXi que admitan E/S de DirectPath.
- Es posible configurar hasta 10 puertos en total; esta es una limitación de VMware. Se utilizará uno para el tráfico de gestión y hasta 9 para el tráfico de datos.
- Únicamente se admite el controlador vmxnet3.
- Los sistemas virtuales no son compatibles.
- vMotion del cortafuegos no es compatible.
- No se admiten tramas gigantes.
- La agregación de enlaces debe estar habilitada en el host ESXi.

Instale un Cortafuegos VM-Series en el hipervisor vSphere de VMware (ESXi)

Para instalar un cortafuegos VM-Series debe tener acceso a la plantilla de formato abierto de virtualización (OVF). Use el código de autenticación que recibió con el correo electrónico de cumplimentación del pedido para registrar su cortafuegos VM-Series y recuperar el acceso a la plantilla de OVF. El OVF se descarga como archivo comprimido zip que se expande en tres archivos: la extensión .ovf es para el archivo descriptor OVF que contiene todos los metadatos del paquete y su contenido; la extensión .mf es para el archivo de manifiesto OVF que contiene los resúmenes SHA-1 de los archivos individuales del paquete, y la extensión .vmdk se aplica al archivo de imagen de disco virtual que contiene la versión virtualizada del cortafuegos.

- Aprovisionamiento del cortafuegos VM-Series en un servidor ESXi
- Configuración inicial en VM-Series en ESXi

Aprovisionamiento del cortafuegos VM-Series en un servidor ESXi

Siga estas instrucciones para implementar el cortafuegos VM-Series en un servidor ESXi (independiente). Para implementar el cortafuegos VM-Series edición NSX, consulte Configuración del cortafuegos VM-Series edición NSX.

Aprovisionamiento del cortafuegos VM-Series		
Paso 1	Descargue el archivo zip que contiene la plantilla de OVF.	Registre su cortafuegos VM-Series y obtenga la plantilla de OVF de: https://support.paloaltonetworks.com. Los archivos anteriores contienen la instalación básica. Cuando la instalación básica haya finalizado, deberá descargar e instalar la versión más reciente de PAN-OS desde el sitio web de asistencia técnica. Con ello garantizará que cuenta con los ajustes más recientes implementados desde la creación de la imagen básica. Para obtener instrucciones, consulte Actualización de la versión de software de PAN-OS (versión independiente).

Aprovisionamiento del cortafuegos VM-Series (Continuación)		
Paso 2	Antes de implementar la plantilla de OVF, configure los conmutadores estándar virtuales y conmutadores distribuidos virtuales que necesitará para el Cortafuegos VM-Series. Si está implementando el Cortafuegos VM-Series con capa 2, cable virtual o interfaces tap, cualquier conmutador virtual adjunto debe permitir los siguientes modos (establecer en Aceptar): – Modo promiscuo – Cambios de direcciones MAC – Transmisiones falsificadas – Para obtener más información, consulte los requisitos de interfaz de red en Requisitos.	**Para configurar un conmutador estándar virtual con el objetivo de recibir tramas para el cortafuegos VM-Series:** 1. Configure un conmutador estándar virtual desde el cliente vSphere desplazándose hasta **Inicio > Inventario > Hosts y clústeres**. 2. Haga clic en la ficha **Configuración** y, bajo **Hardware**, haga clic en **Redes**. Para cada conmutador virtual conectado al Cortafuegos VM-Series, haga clic en **Propiedades**. 3. Resalte el conmutador virtual y haga clic en **Editar**. En las propiedades de vSwitch, haga clic en la pestaña **Seguridad** y establezca **Modo promiscuo, Cambios de dirección MAC** y **Transmisiones falsificadas** en **Aceptar**; a continuación, haga clic en **ACEPTAR**. Este cambio se propagará a todos los grupos de puertos del conmutador virtual. **Para configurar un conmutador distribuido virtual con el objetivo de recibir tramas para el cortafuegos VM-Series:** 1. Seleccione **Inicio > Inventario > Red**. Resalte el **Grupo de puertos distribuido que desee editar y seleccione la ficha Resumen**. 2. Haga clic en **Editar configuración** y seleccione **Políticas > Seguridad**; a continuación, establezca **Modo promiscuo, cambios en direcciones MAC** y **Transmisiones falsificadas** en **Aceptar**; haga clic en **ACEPTAR**.

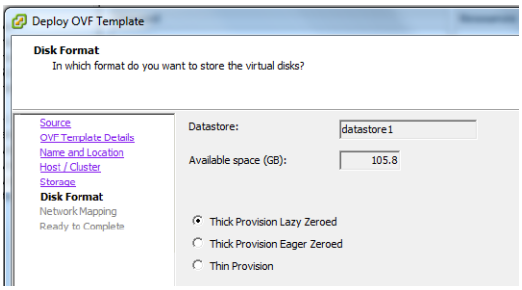
Aprovisionamiento del cortafuegos VM-Series (Continuación)

Paso 3 Implemente la plantilla de OVF.

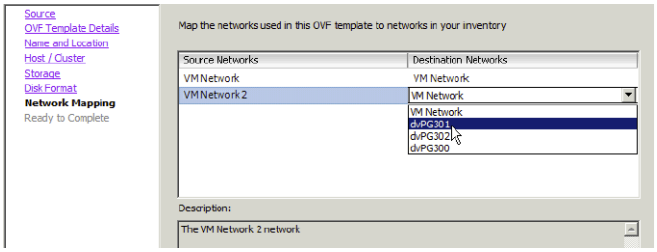
Si añade interfaces adicionales (vmNIC) al cortafuegos VM-Series, debe reiniciar porque las nuevas interfaces se detectan durante el ciclo de inicio. Para evitar tener que reiniciar el cortafuegos, añada las interfaces durante la implementación inicial o durante un periodo de mantenimiento para que pueda reiniciar el cortafuegos.

Para ver el progreso de la instalación, supervise la lista **Tareas recientes**.

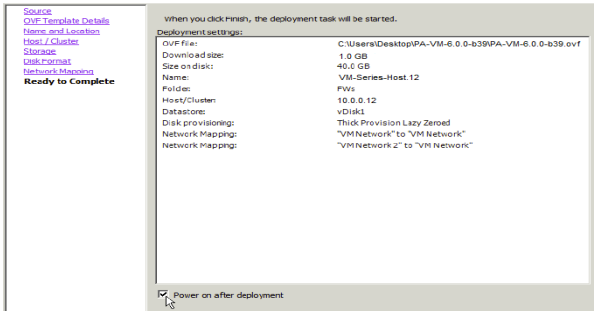
1. Inicie sesión en vCenter mediante el cliente vSphere. También puede ir directamente al host ESXi de destino si es necesario.
2. Desde el cliente vSphere, seleccione **Archivo > Implementar plantilla de OVF**.
3. Desplácese hasta la plantilla de OVF que descargó en el Paso 1, seleccione el archivo y, a continuación, haga clic en **Siguiente**. Revise la ventana de información detallada de las plantillas y, a continuación, vuelva a hacer clic en **Siguiente**.
4. Asigne un nombre a la instancia del Cortafuegos VM-Series y, en la ventana **Ubicación de inventario**, seleccione un centro de datos y carpeta y haga clic en **Siguiente**
5. Seleccione un host ESXi para el Cortafuegos VM-Series y haga clic en **Siguiente**.
6. Seleccione el almacén de datos que se utilizará para el Cortafuegos VM-Series y haga clic en **Siguiente**.
7. Deje la configuración predeterminada para el suministro del almacén de datos y haga clic en **Siguiente**. El valor predeterminado es **Thick Provision Lazy Zeroed**.



8. Seleccione las redes que se utilizarán para las dos vmNIC iniciales. La primera vmNIC se utilizará para la interfaz de gestión y la segunda vmNIC para el primer puerto de datos. Asegúrese de que las **Redes de origen** se asignan a las **Redes de destino** correctas.



9. Revise la ventana de información detallada, haga clic en la casilla de verificación **Activación tras implementación** y, a continuación, haga clic en **Siguiente**.



10. Cuando haya finalizado la implementación, haga clic en la ficha **Resumen** para revisar el estado actual.

Configuración inicial en VM-Series en ESXi

Utilice la consola del dispositivo virtual en el servidor ESXi para configurar el acceso de red al cortafuegos VM-Series. Primero debe configurar la interfaz de gestión y después acceder a la interfaz web para completar más tareas de configuración. Si usa Panorama para la gestión central, consulte la Guía del administrador de Panorama para saber más sobre la gestión del dispositivo mediante Panorama.

Configuración de la interfaz de gestión		
Paso 1	Obtenga la información necesaria de su administrador de red.	• Dirección IP para el puerto MGT • Máscara de red • Puerta de enlace predeterminada • Dirección IP de servidor DNS
Paso 2	Acceda a la consola del cortafuegos VM-Series.	1. Seleccione la ficha **Consola** en el servidor ESXi para el cortafuegos VM-Series o haga clic en el botón derecho del cortafuegos VM-Series y seleccione **Abrir consola**. 2. Pulse Intro para acceder a la pantalla de inicio de sesión. 3. Introduzca el nombre de usuario/contraseña predeterminados (admin/admin) para iniciar sesión. 4. Introduzca **`configurar`** para pasar al modo de configuración.
Paso 3	Defina la configuración de acceso a la red para la interfaz de gestión.	Introduzca el siguiente comando: `set deviceconfig system ip-address <IP-cortafuegos> netmask <máscara de red> default-gateway <IP-puerta de enlace> dns-setting servers primary <IP-DNS>` donde `<IP-cortafuegos>` es la dirección IP que quiere asignar a la interfaz de gestión, `<máscara de red>` es la máscara de subred, `<IP-puerta de enlace>` es la dirección IP de la puerta de enlace de la red y `<IP-DNS>` es la dirección IP del servidor DNS.
Paso 4	Confirme los cambios y salga del modo de configuración.	Introduzca **`commit.`** Introduzca **`exit`**.

Paso 5	Verifique el acceso a la red para los servicios externos requeridos para la gestión del cortafuegos, como el servidor de actualizaciones de Palo Alto Networks.	Para verificar que el cortafuegos tiene acceso de red externa, utilice la utilidad ping utility. Compruebe la conectividad a la puerta de enlace predeterminada, servidor DNS y el servidor de actualización de Palo Alto Networks como se muestra en el siguiente ejemplo:
		`admin@VM_200-Corp> ping host updates.paloaltonetworks.com`
		`Haciendo ping a updates.paloaltonetworks.com (67.192.236.252) con 56(84) bytes de datos.`
		`64 bytes desde 67.192.236.252: icmp_seq=1 ttl=243 tiempo=40.5 ms`
		`64 bytes desde 67.192.236.252: icmp_seq=1 ttl=243 tiempo=53.6 ms`
		`64 bytes desde 67.192.236.252: icmp_seq=1 ttl=243 tiempo=79.5 ms`
		Cuando haya comprobado la conectividad, pulse Ctrl+C para detener los pings.

Un cortafuegos VM-Series sin licencia puede procesar hasta 200 sesiones simultáneas. En función del entorno, el límite de sesiones se puede alcanzar muy rápidamente. Por ello, aplique el código de autenticación de capacidad y recupere una licencia antes de comenzar a probar el cortafuegos VM-Series; de lo contrario puede obtener resultados impredecibles si hay otro tráfico en el grupo de puertos.

Solución de problemas de implementaciones de ESXi

Muchos de los pasos de solución de problemas para el Cortafuegos VM-Series son muy parecidos a los de las versiones de hardware de PAN-OS. Si se produce algún problema, debería comprobar los contadores de la interfaz y archivos de log de sistema y, si es necesario, utilizar la depuración para crear capturas. Si desea más información sobre la solución de problemas de PAN-OS, consulte el artículo de solución de problemas basados en paquetes.

La siguientes secciones describen cómo solucionar algunos problemas comunes:

- Solución de problemas básicos
- Problemas de instalación
- Problemas de licencia
- Problemas de conectividad

Solución de problemas básicos

Recomendación de herramientas de solución de problemas de red

Resulta útil tener una estación de solución de problemas aparte para capturar el tráfico o inyectar paquetes de prueba en el entorno virtualizado. Puede ser útil crear un SO nuevo desde cero con las herramientas de solución de los problemas más comunes instaladas, como tcpdump, nmap, hping, traceroute, iperf, tcpedit, netcat, etc. A continuación esta máquina puede apagarse y convertirse en una plantilla. Cada vez que se necesiten herramientas, el cliente de solución de problemas (máquina virtual) puede implementarse rápidamente en el conmutador virtual en cuestión y usarse para aislar problemas de redes. Cuando la prueba esté completa, la instancia podrá simplemente descartarse y la plantilla se volverá a usar la siguiente vez que sea necesaria.

Para problemas relacionados con el rendimiento en el cortafuegos, primero compruebe el **Panel** en la interfaz web del cortafuegos. Para ver alertas o crear un archivo de asistencia técnica o de volcado de estadísticas, desplácese a **Dispositivo > Asistencia técnica**.

Para obtener información del cliente vSphere, vaya a **Inicio > Inventario > VM y plantillas**, seleccione la instancia del Cortafuegos VM-Series y haga clic en la ficha **Resumen**. Bajo **Recursos**, compruebe las estadísticas de la memoria consumida, la CPU y el almacenamiento. Para conocer el historial de recursos, haga clic en la ficha **Rendimiento** y supervise el consumo de recursos a lo largo del tiempo.

Problemas de instalación

Problemas con la implementación del OVF

VM-Series se proporciona como un archivo descargable de formato abierto de virtualización (OVF). El OVF se descarga como un archivo zip que se extrae en tres carpetas. Si tiene problemas para implementar el OVF, asegúrese de que los tres archivos se extraen y muestran y, si es necesario, vuelva a descargar y extraer el OVF de nuevo.

- La extensión OVF es el archivo descriptivo de OVF que contiene todos los metadatos sobre el paquete y su contenido.
- La extensión MF es el archivo de manifiesto de OVF que contiene los resúmenes de SHA-1 de los archivos individuales del paquete.
- La extensión vmdk es para el archivo de imagen de disco virtual.
- El disco virtual del OVF es grande para VM-Series; este archivo tiene casi 900 MB y debe estar presente en el equipo que ejecuta el cliente vSphere o se debe poder acceder al mismo como una URL del OVF. Asegúrese de que la conexión de red es suficiente entre el ordenador cliente de vSphere y el host ESXi de destino. Los cortafuegos de la ruta deben admitir los puertos TCP 902 y 443 del cliente vSphere al host ESXi. Debe haber suficiente ancho de banda y una baja latencia en la conexión, ya que de lo contrario la implementación del OVF puede tardar horas o agotar el tiempo de espera y fallar.

¿Por qué el cortafuegos se inicia en modo de mantenimiento?

Si ha adquirido la licencia del VM-1000-HV y está implementando el cortafuegos VM-Series en modo independiente en un servidor ESXi de VMware o un servidor SDX de Citrix, debe asignar un mínimo de 5 GB de memoria en el cortafuegos VM-Series.

Para solucionar este problema, debe modificar el archivo de imagen base (consulte ¿Cómo puedo modificar el archivo de imagen base de la licencia de VM-1000-HV?) o edite los ajustes del host ESXi o el servidor vCenter antes de encender el cortafuegos VM-Series.

Compruebe también que la interfaz es VMXnet3; si establece cualquier otro tipo de interfaz, el cortafuegos se reiniciará en el modo de mantenimiento.

¿Cómo puedo modificar el archivo de imagen base de la licencia de VM-1000-HV?

Si ha adquirido la licencia del VM-1000-HV y está implementando el cortafuegos VM-Series en modo independiente en un servidor ESXi de VMware o en un servidor SDX de Citrix, siga estas instrucciones para modificar los siguientes atributos que se definen en el archivo de imagen base (.ovf o .xva) del cortafuegos VM-Series.

Importante: La modificación de valores distintos de los enumerados aquí invalidará el archivo de imagen base.

Modificación del archivo de imagen base (sólo si se usa la licencia VM-1000-HV en el modo independiente)	
Paso 1	Abra el archivo de imagen base, por ejemplo 6.1.0, con una herramienta de edición de texto como el bloc de notas.

Modificación del archivo de imagen base (sólo si se usa la licencia VM-1000-HV en el modo independiente) (Continuación)

Paso 2 Busque 4096 y cambie la asignación de memoria a 5012 (es decir, 5 GB) aquí :

```
<Item>
        <rasd:AllocationUnits>byte * 2^20</rasd:AllocationUnits>
        <rasd:Description>Memory Size</rasd:Description>
        <rasd:ElementName>4096MB of memory</rasd:ElementName>
        <rasd:InstanceID>2</rasd:InstanceID>
        <rasd:ResourceType>4</rasd:ResourceType>
        <rasd:VirtualQuantity>4096</rasd:VirtualQuantity>
<Item>
        <rasd:AllocationUnits>byte * 2^20</rasd:AllocationUnits>
        <rasd:Description>Memory Size</rasd:Description>
        <rasd:ElementName>5102MB of memory</rasd:ElementName>
        <rasd:InstanceID>2</rasd:InstanceID>
        <rasd:ResourceType>5</rasd:ResourceType>
        <rasd:VirtualQuantity>5012</rasd:VirtualQuantity>
```

Paso 3 Cambie el número de núcleos de CPU virtuales que se asignan de 2 a 4 u 8 como desee para su implementación:

```
    <Item>
            <rasd:AllocationUnits>hertz * 10^6</rasd:AllocationUnits>
            <rasd:Description>Number of Virtual CPUs</rasd:Description>
            <rasd:ElementName>2 virtual CPU(s)</rasd:ElementName>
            <rasd:InstanceID>1</rasd:InstanceID>
            <rasd:ResourceType>3</rasd:ResourceType>
            <rasd:VirtualQuantity>2</rasd:VirtualQuantity>
            <vmw:CoresPerSocket ovf:required="false">2</vmw:CoresPerSocket>
          </Item>
    <Item>
            <rasd:AllocationUnits>hertz * 10^6</rasd:AllocationUnits>
            <rasd:Description>Number of Virtual CPUs</rasd:Description>
            <rasd:ElementName>4 virtual CPU(s)</rasd:ElementName>
            <rasd:InstanceID>1</rasd:InstanceID>
            <rasd:ResourceType>3</rasd:ResourceType>
            <rasd:VirtualQuantity>4</rasd:VirtualQuantity>
            <vmw:CoresPerSocket ovf:required="false">2</vmw:CoresPerSocket>
          </Item>
```

También puede implementar el cortafuegos y antes de activar el cortafuegos VM-Series, editar la asignación de la CPU virtual y la memoria directamente en el host ESXi o el servidor vCenter.

Problemas de licencia

¿Por qué no puedo aplicar la licencia de funciones o asistencia técnica?

¿Ha aplicado el código de autenticación de capacidad en el cortafuegos VM-Series? Antes de que pueda activar la licencia de funciones o asistencia técnica, debe aplicar el código de autenticación de capacidad para que el dispositivo pueda obtener un número de serie. Este número de serie es necesario para activar las otras licencias en el cortafuegos VM-Series.

¿Por qué mi cortafuegos VM-Series clonado no tiene una licencia válida?

VMware asigna una UUID a cada máquina virtual que incluye el cortafuegos VM-Series. Así, cuando un cortafuegos VM-Series se clona, se le asigna una nueva UUID. Como el número de serie y la licencia de cada instancia del cortafuegos de la serie está vinculada a la UUID, si clona el cortafuegos VM-Series con licencia, el cortafuegos resultante no tendrá una licencia válida. Necesitará un nuevo código de autenticación para activar la licencia en el cortafuegos que acaba de implementar. Debe aplicar el código de autenticación de capacidad y una nueva licencia de asistencia técnica para obtener actualizaciones de funcionalidad, asistencia técnica y software en el cortafuegos VM-Series.

¿Si se mueve el cortafuegos VM-Series se invalidará la licencia?

Si mueve el cortafuegos VM-Series manualmente de un host a otro, asegúrese de seleccionar la opción **Se ha movido este invitado** para evitar que se invalide la licencia.

Problemas de conectividad

¿Por qué el cortafuegos VM-Series no recibe tráfico de la red?

En el cortafuegos VM-Series, compruebe los registros de tráfico (**Supervisar > Logs**). Si los logs están vacíos, use el siguiente comando CLI para ver los paquetes de las interfaces del cortafuegos VM-Series:

show counter global filter delta yes

```
Global counters:
Elapsed time since last sampling: 594,544 seconds

--------------------------------------------------------------------------------
Total counters shown: 0
--------------------------------------------------------------------------------
```

En el entorno vSphere, compruebe lo siguiente:

- Compruebe los grupos de puertos y confirme que el cortafuegos y las máquinas virtuales están en el grupo de puertos correcto.

  Asegúrese de que las interfaces se asignan correctamente.

  Adaptador de red 1 = gestión

  Adaptador de red 2= Ethernet1/1

  Adaptador de red 3= Ethernet1/2

  Para cada máquina virtual, compruebe los ajustes para verificar que la interfaz se asigna al grupo de puertos correcto.

- Compruebe que se ha habilitado el modo promiscuo para cada grupo de puertos o para todo el conmutador.

  Como las direcciones MAC de PAN-OS del plano de datos son distintas de las direcciones MAC de VMNIC asignadas por vSphere, el grupo de puertos (o todo el vSwitch) debe estar en modo promiscuo:

- Compruebe la configuración de VLAN en vSphere.

El uso de la configuración VLAN en el grupo de puertos vSphere tiene dos objetivos: determina qué grupos de puertos comparten un dominio de 2 niveles, y determina si se etiquetan los puertos de vínculo superior (802.1Q).

- Compruebe los ajustes de puerto de conmutador físico.

  Si se especifica una Id. de VLAN en un grupo de puertos con puertos de vínculo superior, vSphere usará 802.1Q para etiquetar las tramas salientes. La etiqueta debe coincidir con la configuración del conmutador físico, de lo contrario el tráfico no pasará.

  Compruebe las estadísticas del puerto si usa conmutadores distribuidos virtuales (vDS); los conmutadores estándar no proporcionan estadísticas de puerto

Configuración de un Cortafuegos VM-Series en el servidor Citrix SDX

Para reducir el impacto ecológico y consolidar funciones clave en un único servidor, puede implementar una o varias instancias del cortafuegos VM-Series en el servidor Citrix SDX. La implementación del cortafuegos VM-Series junto con la NetScaler VPX garantiza el suministro de aplicaciones, además de la seguridad de red, disponibilidad, rendimiento y visibilidad.

- Acerca del cortafuegos VM-Series en el servidor SDX
- Requisitos y limitaciones del sistema
- Implementaciones compatibles: Cortafuegos VM Series en Citrix SDX
- Instalación del Cortafuegos VM-Series en el servidor SDX
- Tráfico vertical seguro con el cortafuegos VM-Series
- Tráfico horizontal con el cortafuegos VM-Series

Acerca del cortafuegos VM-Series en el servidor SDX

Se pueden implementar una o varias instancias del cortafuegos VM-Series para garantizar el tráfico horizontal o vertical en la red; son compatibles las interfaces de cable virtual, interfaces de la capa 2 y de la capa 3. Para implementar el cortafuegos, consulte Instalación del Cortafuegos VM-Series en el servidor SDX.

Una vez implementado, el cortafuegos VM-Series funciona de forma sincronizada con la NetScaler VPX (si es necesario), un dispositivo virtual de NetScaler implementado en el servidor SDX. La NetScaler VPX proporciona equilibro de carga y una función de gestión de tráfico y suele implementarse frente a una granja de servidores para facilitar un acceso eficaz a los servidores. Para obtener una visión general completa de las funciones de NetScaler, consulte http:www.citrix.com/netscaler. Cuando VM-Series se utiliza conjuntamente para trabajar con la NetScaler VPX, las funciones complementarias mejoran su gestión del tráfico, el equilibro de la carga y las necesidades de seguridad de la aplicación/red.

Este documento asume su familiaridad con la red y la configuración en la NetScaler VPX. Con el fin de proporcionar contexto para los términos utilizados en esta sección, a continuación presentamos una breve actualización sobre las direcciones de IP propiedad de NetScaler a las que se hace referencia en este documento:

- Direcciones IP de NetScaler (NSIP): NSIP es la dirección IP para el acceso de gestión y sistema general al propio NetScaler y para la comunicación de alta disponibilidad.
- Dirección IP asignada (MIP): Una MIP se utiliza para las conexiones en la parte del servidor. No es la dirección IP de NetScaler. En la mayoría de los casos, cuando NetScaler recibe un paquete, sustituye la dirección IP de origen por una MIP antes de enviar el paquete al servidor. Con los servidores abstraídos de los clientes, NetScaler gestiona las conexiones con mayor eficacia.
- Dirección IP del servidor virtual (VIP): Una VIP es la dirección IP asociada con un servidor. Es la dirección IP pública a la que se conectan los clientes. Puede que una instancia de NetScaler que gestiona una amplia variedad de tráfico tenga muchas VIP configuradas.
- Dirección IP de subred (SNIP): Cuando NetScaler se adjunta a varias subredes, las SNIP se pueden configurar para utilizarse como MIP que proporcionan acceso a estas subredes. Las SNIP pueden estar vinculadas a VLAN e interfaces específicas.

Para obtener ejemplos sobre cómo implementar de forma conjunta el cortafuegos VM-Series y la NetScaler VPX, consulte Implementaciones compatibles: Cortafuegos VM Series en Citrix SDX.

Requisitos y limitaciones del sistema

Esta sección enumera los requisitos y las limitaciones del cortafuegos VM-Series en el servidor Citrix SDX.

▲ Requisitos

▲ Limitaciones

Requisitos

Puede implementar varias instancias del cortafuegos VM-Series en el servidor Citrix SDX. Como todas las instancias del cortafuegos necesitan una asignación de recursos mínima (cantidad de CPU, memoria y espacio en disco) en el servidor SDX, asegúrese de cumplir las especificaciones que aparecen a continuación para garantizar un rendimiento óptimo.

Requisito	Detalles
Plataformas SDX	• 11500, 13500, 14500, 16500, 18500, 20500; • 17550, 19550, 20550, 21550
Versión de SDX	10.1+ 10.1 no es compatible; se necesita una versión de software superior a 10.1.
Versión de Citrix XenServer	6.0.2 o superior
Recursos mínimos del sistema Planee y asigne el número total de interfaces de datos que podría necesitar en el cortafuegos VM-Series. Esta tarea es básica durante la implementación inicial, porque añadir o eliminar interfaces del cortafuegos VM-Series después de la implementación inicial hará que las interfaces de datos (Eth 1/1 y Eth 1/2) del cortafuegos VM-Series reasigne a los adaptadores en el servidor SDX. Todas las interfaces de datos se asignan secuencialmente al adaptador con el valor numérico más bajo. Esta reasignación puede producir un fallo de coincidencia en la configuración del cortafuegos.	• Dos vCPU por Cortafuegos VM-Series. Una se utilizará para el plano de gestión y la otra para el plano de datos. Puede añadir cualquier vCPU en las siguientes combinaciones: 2, 4 u 8 vCPU; se asignan vCPU adicionales al plano de datos. • Dos interfaces de red: una dedicada al tráfico de gestión y otra para el tráfico de datos. Con el tráfico de gestión puede utilizar las interfaces 0/x en el plano de gestión o las interfaces 10/x en el plano de datos. Asigne interfaces de red adicionales para el tráfico de datos, según lo necesite su topología de red. • 4 GB de memoria (5 GB para VM-1000-HV). Cualquier memoria adicional que asigne se utilizará únicamente en el plano de gestión. • 40 GB de espacio de disco virtual. Puede añadir espacio de disco adicional de 40 GB(mínimo) a 2 TB (máximo). El espacio de disco adicional se usa sólo para almacenamiento de logs.

Limitaciones

El Cortafuegos VM-Series implementado en el servidor Citrix SDX tiene las siguientes limitaciones:

- Se puede configurar un máximo de 24 puertos. Se utilizará uno para el tráfico de gestión y hasta 23 para el tráfico de datos.
- No se admiten tramas gigantes.
- No se admite la agregación de enlaces.

En Implementaciones compatibles: Cortafuegos VM Series en Citrix SDX puede consultar las implementaciones compatibles.

Para implementar el cortafuegos, consulte Instalación del Cortafuegos VM-Series en el servidor SDX.

Implementaciones compatibles: Cortafuegos VM Series en Citrix SDX

En las siguientes situaciones, el cortafuegos VM-Series asegura el tráfico destinado a los servidores de la red. Funciona junto con la NetScaler VPX para gestionar el tráfico antes o después de que alcance a la NetScaler VPX.

- Situación 1: Protección del tráfico vertical
- Situación 2: Protección del tráfico horizontal (cortafuegos VM-Series en Citrix SDX)

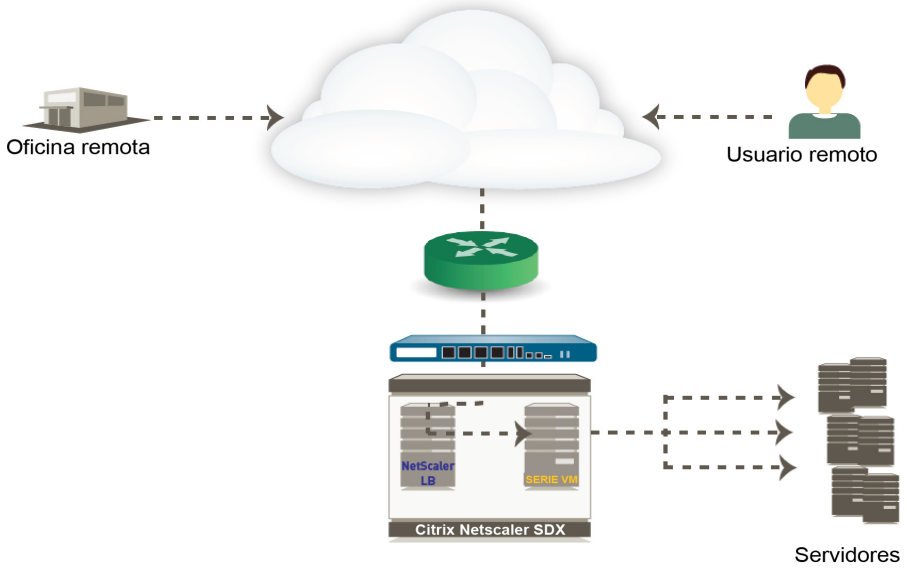
Situación 1: Protección del tráfico vertical

Para proteger el tráfico vertical usando un cortafuegos VM-Series en un servidor SDX, tiene las siguientes opciones:

- Cortafuegos VM-Series entre la NetScaler VPX y los servidores
- Cortafuegos VM-Series antes de la NetScaler VPX

Cortafuegos VM-Series entre la NetScaler VPX y los servidores

El cortafuegos del perímetro acota todo el tráfico en la red. Todo el tráfico permitido en la red fluye a través de la NetScaler VPX y, a continuación, a través del cortafuegos VM-Series antes de que la solicitud se envíe a los servidores.



En esta situación, el cortafuegos VM-Series asegura el tráfico vertical y se puede implementar usando las interfaces de cable virtual, de la capa 2 y la capa 3.

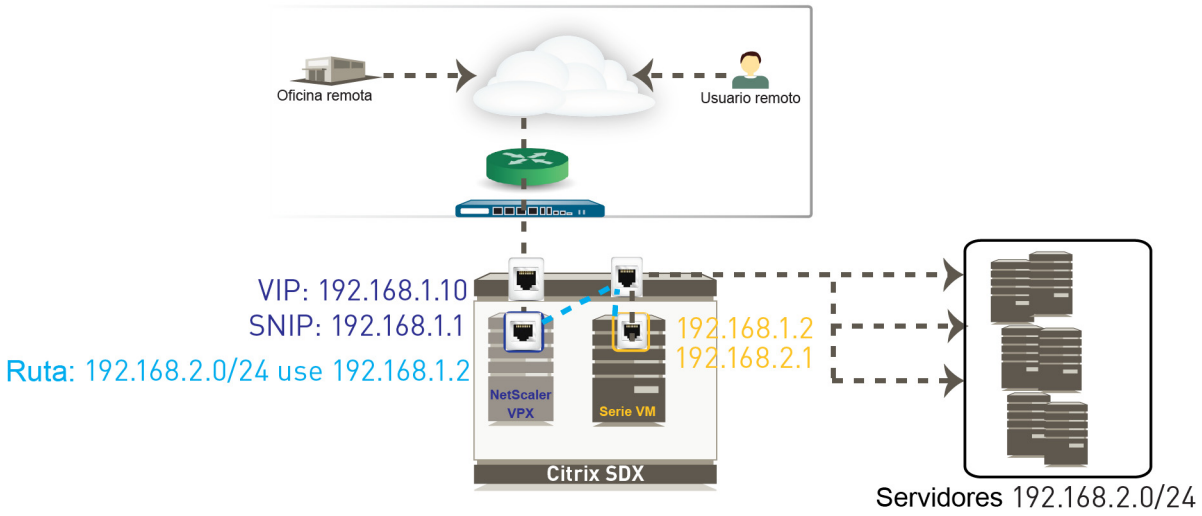
- Cortafuegos VM-Series con interfaces de capa 3
- Cortafuegos VM-Series con interfaces de capa 2 o cable virtual

Cortafuegos VM-Series con interfaces de capa 3

La implementación del cortafuegos con interfaces de capa 3 le permite ampliar capacidad más fácilmente, conforme implemente nuevos servidores y subredes. Puede implementar varias instancias del cortafuegos para gestionar el tráfico a cada nueva subred y, a continuación, configurar los cortafuegos como par de alta disponibilidad, si es necesario.

El uso de una interfaz de L3 le permite realizar cambios mínimos en la configuración de servidor/red de SDC porque la SNIP, para alcanzar los servidores, se elimina de la NetScaler VPX y se configura en el cortafuegos VM-Series. Con este método, sólo se utiliza una interfaz de datos en el cortafuegos VM-Series, por lo que sólo se puede definir una zona. Como resultado, cuando se definen las reglas de la política, debe especificar la dirección IP/subredes de origen y destino en las que aplicar las reglas de seguridad. Para obtener más información, consulte Implementación del cortafuegos VM-Series con interfaces de capa 3.

Topología después de añadir el cortafuegos VM-Series con interfaces de capa 3



En este ejemplo, la dirección IP pública a la que se conecta el cliente (VIP en la NetScaler VPX) es 192.168.1.10. Para proporcionar acceso a los servidores de la subred 192.168.2.x, la configuración de la VPX hace referencia a las subredes (SNIP) 192.168.1.1 y 192.168.2.1. Según su configuración de red y rutas predeterminadas, es posible que deba modificar la ruta de los servidores.

Cuando configura el cortafuegos VM-Series, debe añadir una interfaz de datos (por ejemplo, eth1/1) y asignar dos direcciones IP a la interfaz. Una dirección IP debe estar en la misma subred que la VIP y la otra debe estar en la misma subred que los servidores. En este ejemplo, las direcciones IP asignadas a las interfaces de datos son 192.168.1.2 y 192.168.2.1. Como sólo se utiliza una interfaz de datos en el cortafuegos VM-Series, todo el tráfico pertenece a una única zona y todo el tráfico interno de la zona se permite implícitamente en la política. Por lo tanto, cuando se definen las reglas de la política, debe especificar la dirección IP/subredes de origen y destino en las que aplicar las reglas de seguridad.

Incluso después de que haya añadido el cortafuegos VM-Series al servidor SDX, la dirección IP a la que continúan conectándose los clientes es la VIP de la NetScaler VPX (192.168.1.10). Sin embargo, para dirigir todo el tráfico a través del cortafuegos, debe definir una ruta a la subred 192.168.2.x en la NetScaler VPX. En este ejemplo, para acceder a los servidores, esta ruta debe hacer referencia a la dirección IP 192.168.1.2 asignada

a la interfaz de datos del cortafuegos VM-Series. Ahora, todo el tráfico destinado a los servidores se dirige desde la NetScaler VPX al cortafuegos y, a continuación, a los servidores. El tráfico de retorno utiliza la interfaz 192.168.2.1 en VM-Series y utiliza la SNIP 192.168.1.1 como su siguiente salto.

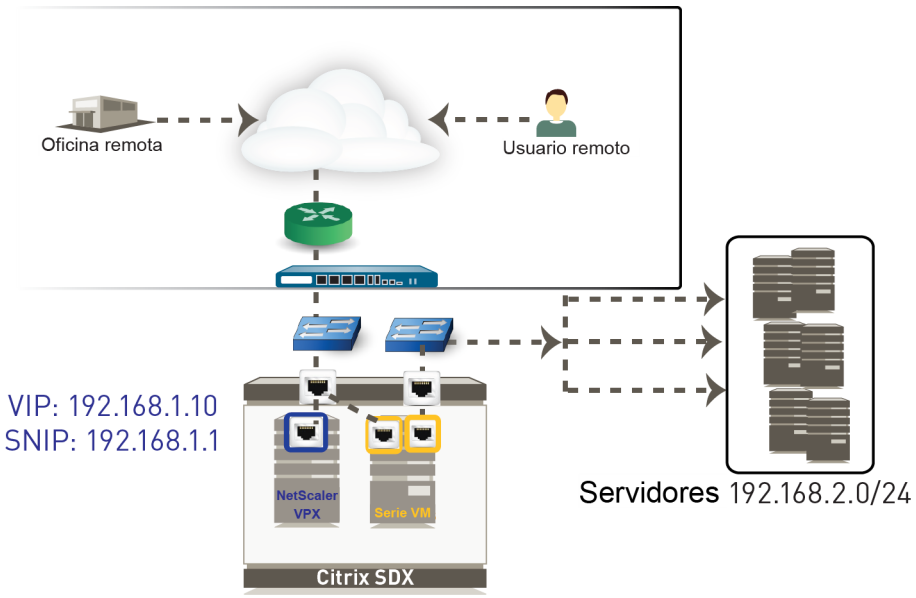
Para cumplir con los requisitos de seguridad, si la opción USIP (Usar IP de origen de cliente) está habilitada en la NetScaler VPX, entonces el cortafuegos VM-Series necesita una ruta predeterminada que apunte a la SNIP 192.168.1.1, en este ejemplo. Si se utiliza una dirección IP de NAT predeterminada (asignada/SNIP), no tendrá que definir una ruta predeterminada en el cortafuegos VM-Series.

Para obtener instrucciones, consulte Implementación del cortafuegos VM-Series con interfaces de capa 3.

Cortafuegos VM-Series con interfaces de capa 2 o cable virtual

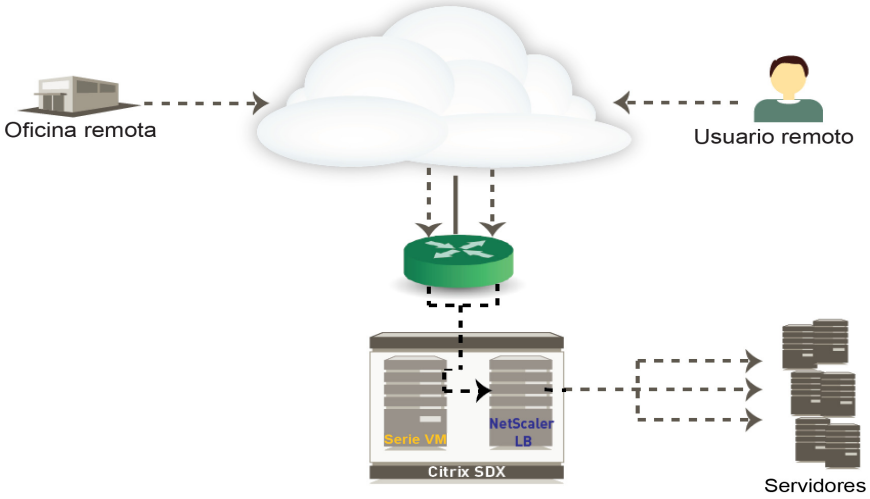
La implementación del cortafuegos VM-Series con interfaces de capa 2 o de cable virtual necesita que reconfigure la NetScaler VPX para eliminar la conexión directa a los servidores. En ese momento, el cortafuegos VM-Series ya se puede cablear y configurar para interceptar de forma transparente y aplicar la política al tráfico destinado a los servidores. En este método, se crean dos interfaces de datos en el cortafuegos, cada una perteneciente a una zona distinta. La política de seguridad se define para permitir el tráfico entre las zonas de origen y destino. Para obtener más información, consulte Implementación del cortafuegos VM-Series con interfaces de capa 2 (L2) o de cable virtual.

Topología después de añadir el cortafuegos VM-Series con interfaces de capa 2 o cable virtual



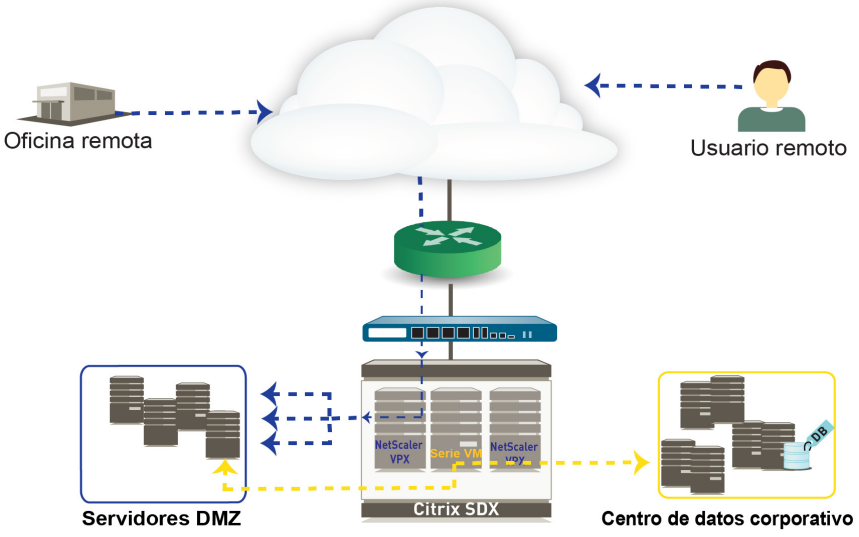
Cortafuegos VM-Series antes de la NetScaler VPX

En esta situación, al cortafuegos del perímetro lo sustituye el cortafuegos VM-Series, que se puede implementar usando las interfaces de cable virtual, de capa 3 o de capa 2. El cortafuegos VM-Series asegura todo el tráfico de la red antes de que la solicitud alcance la NetScaler VPX y se envíe a los servidores. Para obtener más información, consulte Implementación del cortafuegos VM-Series antes de la NetScaler VPX.



Situación 2: Protección del tráfico horizontal (cortafuegos VM-Series en Citrix SDX)

El cortafuegos VM-Series se implementa junto con dos sistemas de la NetScaler VPX que prestan servicio a distintos segmentos del servidor de su red o que funcionan como puntos de terminación para los túneles SSL. En esta situación, el cortafuegos del perímetro garantiza el tráfico entrante. Entonces, el tráfico destinado a los servidores de DMZ fluye a una NetScaler VPX que equilibra las cargas de la solicitud. Para añadir una capa adicional de seguridad a la red interna, todo el tráfico horizontal entre DMZ y la red corporativa se enruta a través del cortafuegos VM-Series. El cortafuegos puede aplicar la seguridad de red y validar el acceso para ese tráfico. Para obtener más información, consulte Tráfico horizontal con el cortafuegos VM-Series.



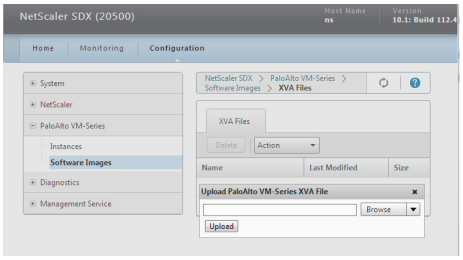
Instalación del Cortafuegos VM-Series en el servidor SDX

Se necesita una cuenta de asistencia y una licencia VM-Series válida para obtener el archivo .xva de imagen base necesario para instalar el cortafuegos VM-Series en el servidor SDX. Si no ha registrado todavía el código de autenticación de capacidad que ha recibido con el correo electrónico de cumplimiento del pedido, con su cuenta de asistencia, consulte Registro del cortafuegos VM-Series. Después de completar el registro, continúe realizando las siguientes tareas:

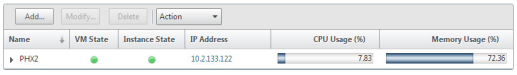
- Carga de la imagen en el servidor SDX
- Aprovisionamiento del cortafuegos VM-Series en el servidor SDX

Carga de la imagen en el servidor SDX

Para aprovisionar el cortafuegos VM-Series, debe obtener el archivo de imagen .xva y cargarlo al servidor SDX.

Carga de la imagen XVA en el servidor SDX	
Paso 1 Descargue y extraiga el archivo .zip de imagen base en un ordenador local.	1. Vaya a https://support.paloaltonetworks.com/ y descargue el archivo .zip de **imagen base de Citrix SDX VM-Series**. 2. Descomprima el archivo zip de la imagen base y extraiga el archivo **.xva**. Este archivo .xva es necesario para instalar el cortafuegos VM-Series.
Paso 2 Cargue la imagen del ordenador local al servidor Citrix SDX.	1. Inicie el navegador web e inicie sesión en el servidor SDX. 2. Seleccione **Configuración > VM-Series de Palo Alto > Imágenes de software** 3. En el menú desplegable **Acción**, seleccione **Cargar**... y **navegue** hasta la ubicación del archivo de imagen *.xva* guardado. 4. Seleccione la imagen y haga clic en **Abrir**. 5. **Cargue** la imagen en el servidor SDX. 

Aprovisionamiento del cortafuegos VM-Series en el servidor SDX

Aprovisionamiento del cortafuegos VM-Series en el servidor SDX		
Paso 1	Acceda al servidor SDX.	Inicie el navegador web y conecte al servidor SDX.
Paso 2	Cree el cortafuegos VM-Series. Asigne el número total de interfaces de datos que podría necesitar en el cortafuegos VM-Series durante la implementación inicial. Añadir o eliminar interfaces al cortafuegos VM-Series después de la implementación inicial hará que las interfaces de datos (Eth 1/1 y Eth 1/2) del cortafuegos VM-Series reasigne a los adaptadores en el servidor SDX. Cada interfaz de datos asigna secuencialmente al adaptador el valor numérico más bajo y puede, por tanto, producir un fallo de coincidencia en la configuración del cortafuegos.	1. Seleccione **Configuración > VM-Series de Palo Alto > Instancias** 2. Haga clic en **Añadir**. 3. Introduzca un nombre para el cortafuegos VM-Series. 4. Seleccione la imagen .xva que había cargado anteriormente. Esta imagen es necesaria para abastecer el cortafuegos. 5. Asigne memoria, espacio en disco adicional y CPU virtuales para el cortafuegos VM-Series. Para verificar las recomendaciones de asignación de recursos, consulte Requisitos. 6. Seleccione las interfaces de red: • Utilice las interfaces de gestión 0/1 o 0/2 y asigne una dirección IP, una máscara de red y una dirección IP de puerta de enlace. Si es necesario, puede utilizar una interfaz de datos en el servidor SDX para gestionar el cortafuegos. • Seleccione las interfaces de datos que se utilizarán para gestionar el tráfico hacia y desde el cortafuegos. Si planea implementar las interfaces como capa 2 o de cable virtual, seleccione la opción **Permitir modo de capa 2** de forma que el cortafuegos pueda recibir y reenviar los paquetes para direcciones MAC que no sean las propias.  7. Revise el resumen y haga clic en **Finalizar** para comenzar el proceso de instalación. Lleva 5-8 minutos aprovisionar el cortafuegos. Cuando termine, utilice la dirección IP de gestión para iniciar la interfaz web del cortafuegos.

Continúe con el Activación de la licencia.

Tráfico vertical seguro con el cortafuegos VM-Series

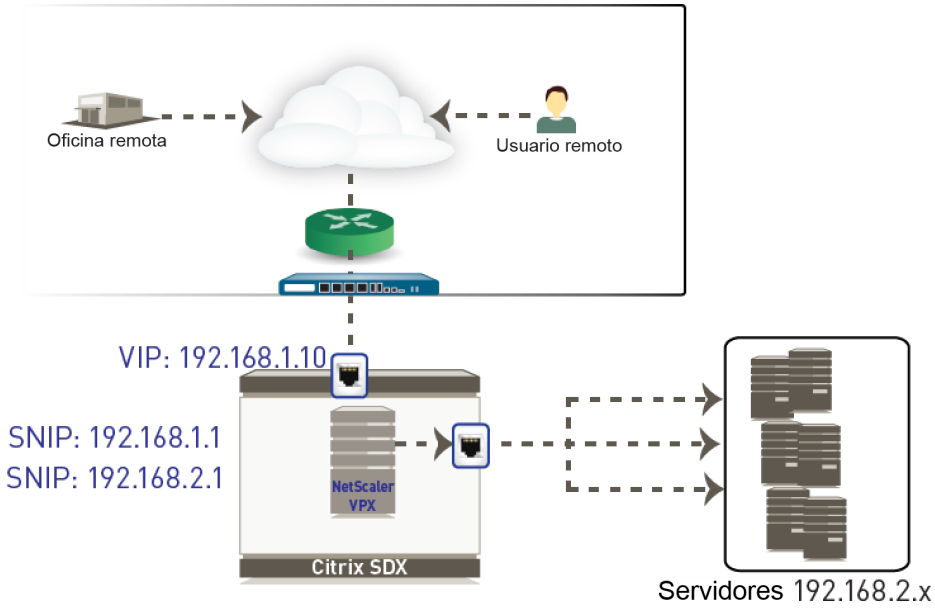
Esta sección incluye información sobre la implementación de NetScaler VPX y el cortafuegos VM-Series en el servidor Citrix SDX:

- Implementación del cortafuegos VM-Series con interfaces de capa 3
- Implementación del cortafuegos VM-Series con interfaces de capa 2 (L2) o de cable virtual
- Implementación del cortafuegos VM-Series antes de la NetScaler VPX (con interfaces de cable virtual)

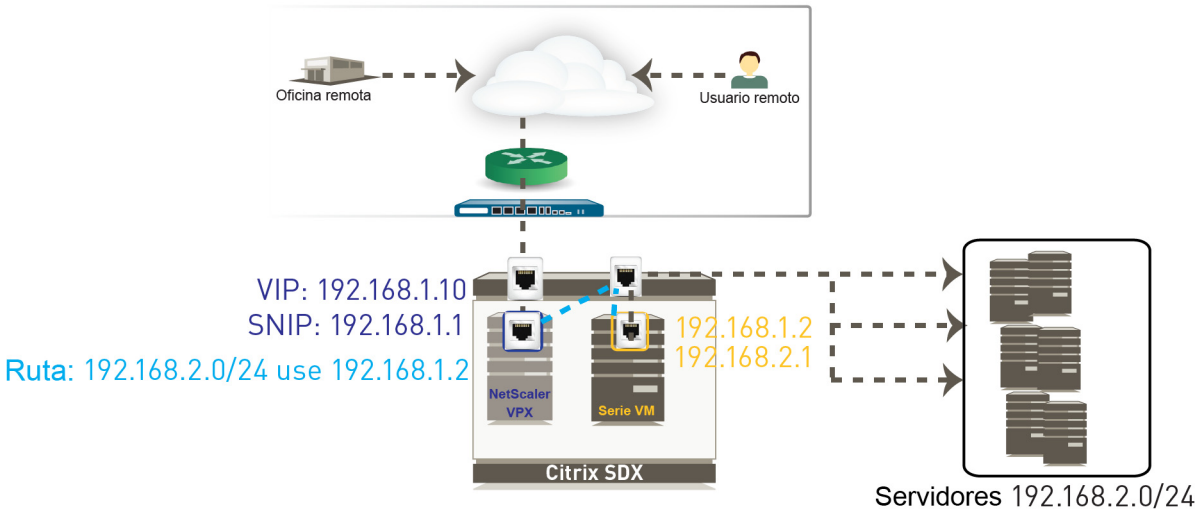
Implementación del cortafuegos VM-Series con interfaces de capa 3

Para asegurar el tráfico vertical, esta situación le muestra cómo implementar el cortafuegos VM-Series con capa 3; el cortafuegos VM-Series se coloca para asegurar el tráfico entre la NetScaler VPX y los servidores de la red.

Topología antes de añadir el cortafuegos VM-Series



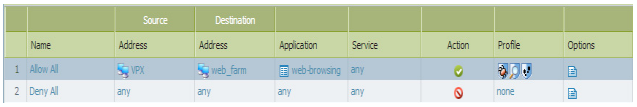
Topología después de añadir el cortafuegos VM-Series



En la siguiente tabla se incluyen las tareas que debe realizar para implementar el cortafuegos VM-Series. En la documentación de PAN-OS puede consultar las instrucciones de configuración del cortafuegos. El flujo de trabajo y la configuración de la NetScaler VPX no se explican en este documento; para obtener más información sobre cómo configurar la NetScaler VPX, consulte la documentación de Citrix.

Configuración del cortafuegos VM-Series para procesar tráfico vertical usando las interfaces de la capa 3		
Paso 1	Instalación del Cortafuegos VM-Series en el servidor SDX.	Cuando aprovisiona el cortafuegos VM-Series en el servidor SDX, debe asegurarse de seleccionar la interfaz de datos con precisión para que el cortafuegos pueda acceder a los servidores.
Paso 2	Configure la interfaz de datos en el cortafuegos.	1. Seleccione **Red > Enrutador virtual** y, a continuación, seleccione el enlace **predeterminado** para abrir el cuadro de diálogo Enrutador virtual y **añada** la interfaz al enrutador virtual. 2. (Solo es necesario si la opción USIP está habilitada en la NetScaler VPX) En la ficha **Rutas estáticas** del enrutador virtual, seleccione la interfaz y añada la NetScaler SNIP (192.68.1.1 en este ejemplo) como **Siguiente salto**. La ruta estática definida aquí se utilizará para dirigir el tráfico desde el cortafuegos hasta la NetScaler VPX. 3. Seleccione **Red > Interfaces > Ethernet** y, a continuación, seleccione la interfaz que quiera configurar. 4. Seleccione el **Tipo de interfaz**. Aunque su decisión aquí depende de la topología de su red, este ejemplo utiliza **Capa3**. 5. En la ficha **Configuración**, en el menú desplegable **Enrutador virtual**, seleccione **predeterminado**. 6. Seleccione **Nueva zona** en el menú desplegable **Zona de seguridad**. En el cuadro de diálogo Zona, defina un **Nombre** para una nueva zona, por ejemplo "Predeterminado" y, a continuación, haga clic en **Aceptar**. 7. Seleccione la ficha **IPv4 o IPv6**, haga clic en **Añadir** en la sección IP e introduzca las dos direcciones IP y la máscara de red para la interfaz (una para cada subred a la que se esté dando servicio). Por ejemplo, 192.168.1.2 y 192.168.2.1. 8. (Optativo) Para permitirle hacer ping o usar SSH en la interfaz, seleccione **Avanzada > Otra información**, abra el menú desplegable **Perfil de gestión** y seleccione el **Nuevo perfil de gestión**. Introduzca un **nombre** para el perfil, seleccione **Ping** y **SSH** y, a continuación, haga clic en **Aceptar**. 9. Para guardar la configuración de la interfaz, haga clic en **Aceptar**. 10. Haga clic en **Compilar** para guardar sus cambios en el cortafuegos.

Configuración del cortafuegos VM-Series para procesar tráfico vertical usando las interfaces de la capa 3 (Continuación)

Paso 3 Cree una política básica que permita el tráfico entre la NetScaler VPX y los servidores web. En este ejemplo, debido a que sólo hemos configurado una interfaz de datos, especificamos la dirección IP de destino y de origen para permitir el tráfico entre la NetScaler VPX y los servidores.	1. Seleccione **Políticas > Seguridad** y haga clic en **Añadir**. 2. Asigne a la regla un nombre descriptivo en la pestaña **General**. 3. En la ficha **Origen**, seleccione **Añadir** en la sección Dirección de origen y seleccione el enlace de nueva **dirección**. 4. Cree un objeto de nueva dirección que especifique la SNIP en la NetScaler VPX. En este ejemplo, esta dirección IP es el origen de todas las solicitudes para los servidores. 5. En la ficha **Destino**, seleccione **Añadir** en la sección Dirección de destino y seleccione el enlace de nueva **dirección**. 6. Cree un objeto de nueva dirección que especifique la subred de los servidores web. En este ejemplo, esta subred alberga todos los servidores web que atienden las solicitudes. 7. En la ficha **Aplicación**, seleccione la navegación web. 8. En la pestaña **Acciones**, realice estas tareas: a. Establezca **Configuración de acción** como **Permitir**. b. Adjunte los perfiles predeterminados para la protección antivirus y contra vulnerabilidades dentro de **Ajuste de perfil**. 9. Verifique que los logs están habilitados al final de una sesión bajo **Opciones**. Únicamente se registrará el tráfico que coincida con una regla de seguridad.  10. Cree otra regla para denegar cualquier otro tráfico de cualquier dirección IP de origen y de destino de la red. Como todo el tráfico interno de la zona está permitido de forma predeterminada, para poder denegar tráfico no relacionado con la navegación web, debe crear una regla de denegación que bloquee explícitamente el resto del tráfico.

Vuelva a Tráfico vertical seguro con el cortafuegos VM-Series o consulte Tráfico horizontal con el cortafuegos VM-Series.

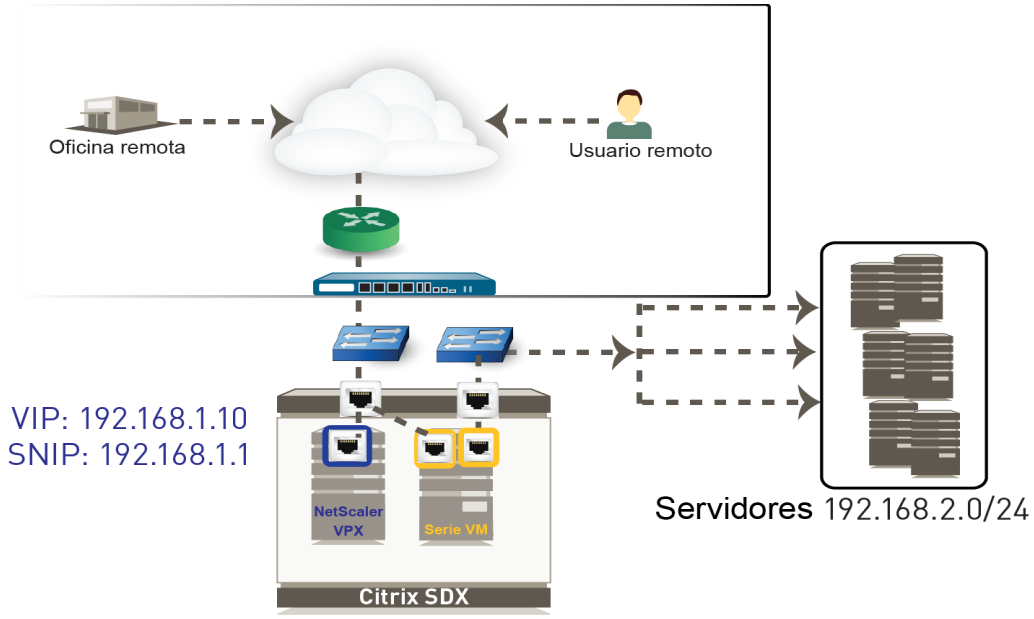
Para obtener información general sobre las implementaciones, consulte Implementaciones compatibles: Cortafuegos VM Series en Citrix SDX.

Implementación del cortafuegos VM-Series con interfaces de capa 2 (L2) o de cable virtual

Para asegurar el tráfico vertical, esta situación le muestra cómo implementar el cortafuegos VM-Series en una implementación de capa 2 o de cable virtual. El cortafuegos VM-Series asegura el tráfico destinado a los servidores. La solicitud llega a la dirección VIP de la NetScaler VPX y la procesa el cortafuegos VM-Series antes de que alcance los servidores. En la ruta de retorno, el tráfico se dirige a la SNIP en la NetScaler VPX y el cortafuegos VM-Series lo procesa antes de que el cliente lo reciba de vuelta.

Para conocer la topología antes de añadir el cortafuegos VM-Series, consulte Topología antes de añadir el cortafuegos VM-Series.

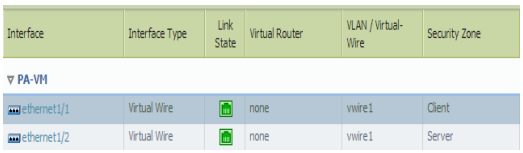
Topología después de añadir el cortafuegos VM-Series



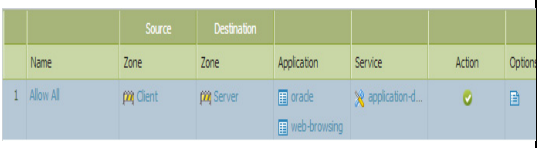
En la siguiente tabla se incluyen las tareas básicas de configuración que debe realizar para implementar el cortafuegos VM-Series. En la documentación de PAN-OS puede consultar las instrucciones de configuración del cortafuegos. El flujo de trabajo y la configuración de la NetScaler VPX no se explican en este documento; para obtener más información sobre cómo configurar la NetScaler VPX, consulte la documentación de Citrix.

Configuración del cortafuegos VM-Series para procesar tráfico vertical usando la interfaces de la capa 2 o cable virtual	
Paso 1 Instalación del Cortafuegos VM-Series en el servidor SDX.	En el servidor SDX, asegúrese de habilitar **Permitir modo de capa 2** en todas las interfaces de datos. Este ajuste permite al cortafuegos sortear paquetes destinados a la VIP de NetScaler VPX.

Configuración del cortafuegos VM-Series para procesar tráfico vertical usando la interfaces de la capa 2 o cable virtual (Continuación)

Paso 2 Vuelva a conectar el cable a la interfaz de la parte del servidor asignada a la NetScaler VPX. Como la NetScaler VPX se reiniciará cuando vuelva a conectarse el cable, evalúe si desea realizar esta tarea durante una ventana de mantenimiento.	Si ya ha implementado una NetScaler VPX y ahora está añadiendo el cortafuegos VM-Series al servidor SDX, tendrá dos puertos asignados a la VPX. Cuando implemente el cortafuegos VM-Series, la NetScaler VPX sólo necesitará un puerto para gestionar el tráfico de la parte del cliente. Por lo tanto, antes de configurar las interfaces de datos VM-Series, debe retirar el cable de la interfaz que conecta la VPX a la granja de servidores y conectarlo al cortafuegos para que este procese todo el tráfico dirigido a la granja de servidores.
Paso 3 Configure las interfaces de datos. En este ejemplo se muestra la configuración para las interfaces de cable virtual.  	1. Inicie la interfaz web del cortafuegos. 2. Seleccione **Red > Interfaces > Ethernet**. 3. Haga clic en el enlace de una interfaz (por ejemplo, ethernet 1/1) y seleccione el **tipo de interfaz** como de **capa 2** o **cable virtual**. **Configuración de cable virtual** Todas las interfaces de cable virtual (ethernet 1/1 y ethernet 1/2) deben conectarse a una zona de seguridad y un cable virtual. Para configurar estos ajustes, seleccione la ficha **Configuración** y complete las siguientes tareas: a. En el menú desplegable Cable virtual haga clic en **Nuevo cable virtual**, defina un **nombre**, asígnele las dos interfaces de datos (ethernet 1/1 y ethernet 1/2) y, a continuación, haga clic en **Aceptar**. Cuando configure ethernet 1/2, seleccione este cable virtual. b. Seleccione **Nueva zona** en el menú desplegable **Zona de seguridad**, defina un **nombre** para la nueva zona, por ejemplo *cliente* y, a continuación, haga clic en **Aceptar**. **Configuración de capa 2** Necesita una zona de seguridad en cada interfaz de capa 2. Seleccione la ficha **Configuración** y complete las siguientes tareas: a. Seleccione **Nueva zona** en el menú desplegable **Zona de seguridad**, defina un **nombre** para la nueva zona, por ejemplo *cliente* y, a continuación, haga clic en **Aceptar**. 4. Repita los pasos 2 y 3 que aparecen anteriormente para la otra interfaz. 5. Haga clic en **Compilar** para guardar los cambios en el cortafuegos.

Configuración del cortafuegos VM-Series para procesar tráfico vertical usando la interfaces de la capa 2 o cable virtual (Continuación)

Paso 4 Cree una regla de política básica que permita el tráfico a través del cortafuegos. En este ejemplo se muestra cómo permitir el tráfico entre la NetScaler VPX y los servidores web. 	1. Seleccione **Políticas > Seguridad** y haga clic en **Añadir**. 2. Asigne a la regla un nombre descriptivo en la pestaña **General**. 3. En la ficha **Origen**, establezca la **zona de origen** para la zona de la parte del cliente que ha definido. En este ejemplo, seleccione el cliente. 4. En la ficha **Destino**, establezca la **zona de destino** para la zona de la parte del servidor que ha definido. En este ejemplo, seleccione el servidor. 5. En la ficha **Aplicación**, haga clic en **Añadir** para seleccionar las aplicaciones a las que debe permitir el acceso. 6. En la pestaña **Acciones**, realice estas tareas: a. Establezca **Configuración de acción** como **Permitir**. b. Adjunte los perfiles predeterminados para la protección antivirus, antispyware y contra vulnerabilidades y para el filtrado de URL, en **Ajuste de perfil**. 7. Verifique que los logs están habilitados al final de una sesión bajo **Opciones**. Únicamente se registrará el tráfico que coincida con una regla de seguridad.

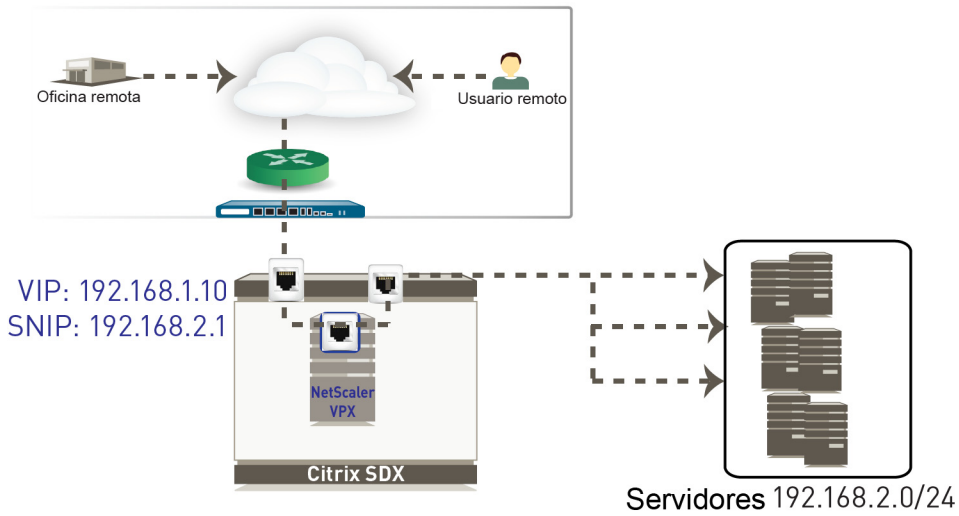
Vuelva a Tráfico vertical seguro con el cortafuegos VM-Series o consulte Tráfico horizontal con el cortafuegos VM-Series.

Para obtener información general sobre las implementaciones, consulte Implementaciones compatibles: Cortafuegos VM Series en Citrix SDX.

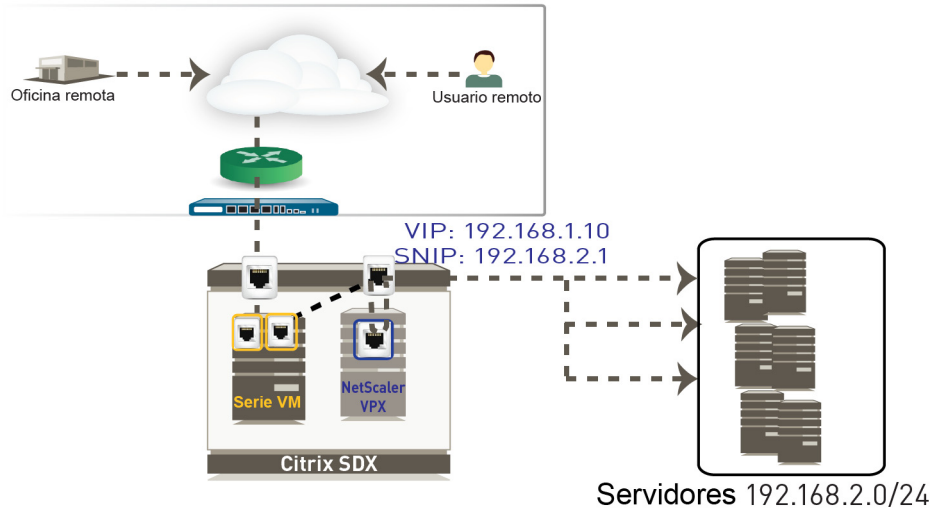
Implementación del cortafuegos VM-Series antes de la NetScaler VPX

En el siguiente ejemplo se muestra cómo implementar el cortafuegos VM-Series para procesar y asegurar el tráfico antes de que alcance la NetScaler VPX. En este ejemplo, el cortafuegos VM-Series se implementa con las interfaces de cable virtual y las solicitudes de conexión del cliente se destinan a la VIP de la NetScaler VPX. Observe que puede implementar el cortafuegos VM-Series usando las interfaces de capa 2 o capa 3, basadas en necesidades específicas.

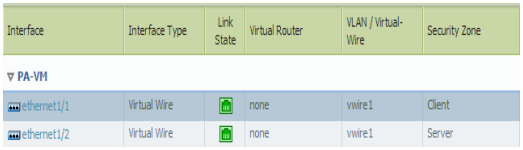
Topología antes de añadir el cortafuegos VM-Series



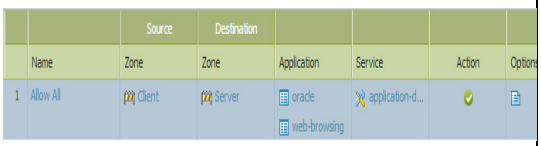
Topología después de añadir el cortafuegos VM-Series



En la siguiente tabla se incluyen las tareas básicas de configuración que debe realizar en el cortafuegos VM-Series. En la documentación de PAN-OS puede consultar las instrucciones de configuración del cortafuegos. El flujo de trabajo y la configuración de la NetScaler VPX no se explican en este documento; para obtener más información sobre cómo configurar la NetScaler VPX, consulte la documentación de Citrix.

Configuración del cortafuegos VM-Series antes de la NetScaler VPX con interfaces de cable virtual	
Paso 1 Instalación del Cortafuegos VM-Series en el servidor SDX.	En el servidor SDX, asegúrese de habilitar **Permitir modo de capa 2** en la interfaz de datos. Este ajuste permite al cortafuegos sortear paquetes destinados a la VIP de NetScaler VPX.
Paso 2 Vuelva a conectar el cable a la interfaz de la parte del cliente asignada a la NetScaler VPX. Como la NetScaler VPX se reiniciará cuando vuelva a conectarse el cable, evalúe si desea realizar esta tarea durante una ventana de mantenimiento.	Si ya ha implementado una NetScaler VPX y ahora está añadiendo el cortafuegos VM-Series al servidor SDX, tendrá dos puertos asignados a la VPX. Cuando implementa el cortafuegos VM-Series, la NetScaler VPX sólo necesitará un puerto que lo conecte a la granja de servidores. Por lo tanto, antes de configurar las interfaces de datos VM-Series, debe retirar el cable de la interfaz que conecta la VPX al tráfico de la parte del cliente y conectarlo al cortafuegos para que este procese todo el tráfico entrante.
Paso 3 Configure las interfaces de datos.  	1. Inicie la interfaz web del cortafuegos. 2. Seleccione **Red > Interfaces > Ethernet**. 3. Haga clic en el enlace de una interfaz (por ejemplo, ethernet 1/1) y seleccione el **tipo de interfaz** como de **cable virtual**. 4. Haga clic en el enlace de la otra interfaz y seleccione el **tipo de interfaz** como de **cable virtual**. 5. Todas las interfaces de cable virtual deben conectarse a una zona de seguridad y un cable virtual. Para configurar estos ajustes, seleccione la ficha **Configuración** y complete las siguientes tareas: • En el menú desplegable Cable virtual haga clic en **Nuevo cable virtual**, defina un **nombre**, asígnele las dos interfaces de datos (ethernet 1/1 y ethernet 1/2) y, a continuación, haga clic en **Aceptar**. Cuando configure ethernet 1/2, seleccione este cable virtual. • Seleccione **Nueva zona** en el menú desplegable **Zona de seguridad**, defina un **nombre** para la nueva zona, por ejemplo cliente y, a continuación, haga clic en **Aceptar**. 6. Repita el paso 5 para la otra interfaz. 7. Haga clic en **Compilar** para guardar los cambios en el cortafuegos.

Configuración del cortafuegos VM-Series antes de la NetScaler VPX con interfaces de cable virtual (Continuación)

Paso 4 Cree una regla de política básica que permita el tráfico a través del cortafuegos. En este ejemplo se muestra cómo permitir el tráfico entre la NetScaler VPX y los servidores web.  	1. Seleccione **Políticas > Seguridad** y haga clic en **Añadir**. 2. Asigne a la regla un nombre descriptivo en la pestaña **General**. 3. En la ficha **Origen**, establezca la **zona de origen** para la zona de la parte del cliente que ha definido. En este ejemplo, seleccione el cliente. 4. En la ficha **Destino**, establezca la **zona de destino** para la zona de la parte del servidor que ha definido. En este ejemplo, seleccione el servidor. 5. En la ficha **Aplicación**, haga clic en **Añadir** para seleccionar las aplicaciones a las que debe permitir el acceso. 6. En la pestaña **Acciones**, realice estas tareas: a. Establezca **Configuración de acción** como **Permitir**. b. Adjunte los perfiles predeterminados para la protección antivirus, antispyware y contra vulnerabilidades y para el filtrado de URL, en **Ajuste de perfil**. 7. Verifique que los logs están habilitados al final de una sesión bajo **Opciones**. Únicamente se registrará el tráfico que coincida con una regla de seguridad.

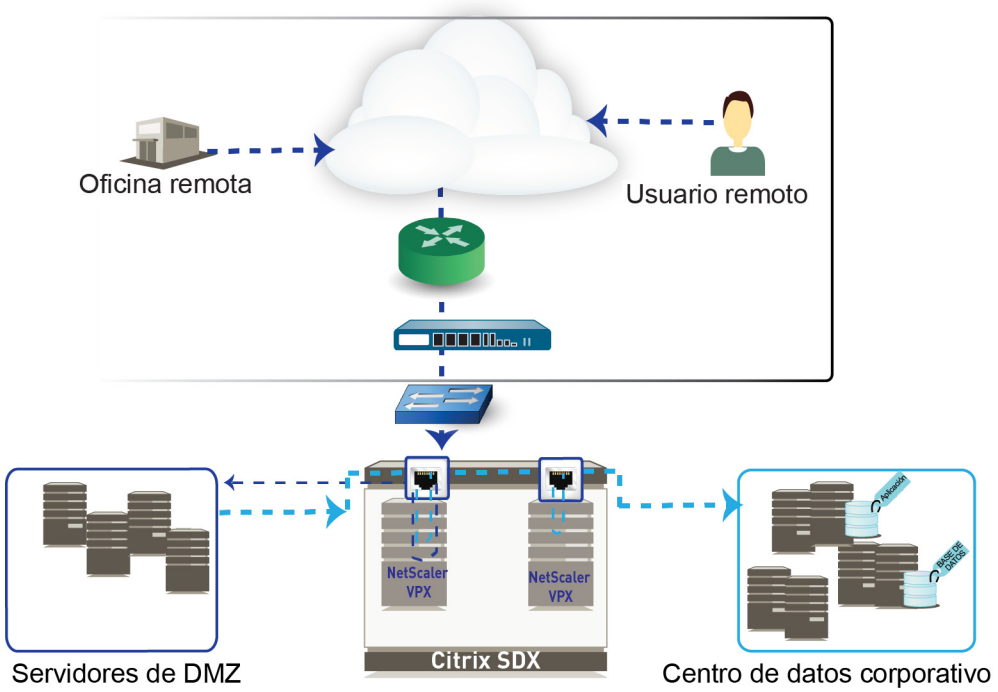
Vuelva a Tráfico vertical seguro con el cortafuegos VM-Series o consulte Tráfico horizontal con el cortafuegos VM-Series.

Para obtener información general sobre las implementaciones, consulte Implementaciones compatibles: Cortafuegos VM Series en Citrix SDX.

Tráfico horizontal con el cortafuegos VM-Series

En el siguiente ejemplo se muestra cómo implementar el cortafuegos VM-Series para asegurar la aplicación o los servidores de la base de datos en su red. Esta situación se le aplica si dispone de dos instancias de la NetScaler VPX, una que autentica a los usuarios, termina las conexiones SSL y, a continuación, equilibra las cargas de las solicitudes en los servidores DMZ y otra que equilibra las cargas de las conexiones con los servidores corporativos que albergan la aplicación y los servidores de bases de datos en su red.

Topología antes de añadir el cortafuegos VM-Series



Ambas instancias de la NetScaler VPX procesan la comunicación entre los servidores de DMZ y los del centro de datos corporativo. Se proporciona una nueva solicitud a la otra instancia de la NetScaler VPX, que envía la solicitud al servidor correspondiente, para el contenido que reside en el centro de datos corporativo.

Cuando el cortafuegos de VM-Series se implementa (este ejemplo utiliza las interfaces de capa 3), el flujo de tráfico es el siguiente:

- Todas las solicitudes entrantes se autentican y la conexión SSL se termina en la primera instancia de la NetScaler VPX. Para obtener el contenido solicitado, si reside en la DMZ, la NetScaler VPX inicia una nueva conexión al servidor. Observe que el tráfico vertical destinado al centro de datos corporativo o a los servidores de la DMZ lo gestiona el cortafuegos perimetral y no el cortafuegos VM-Series.

  Por ejemplo, cuando un usuario (IP de origen 1.1.1.1) solicita contenido desde un servidor de la DMZ, la IP de destino es 20.5.5.1 (VIP de la NetScaler VPX). Entonces, la NetScaler VPX sustituye la dirección IP de destino, basada en el protocolo a la dirección IP del servidor interno, p. ej. 192.168.10.10. El tráfico de retorno desde el servidor se envía de vuelta a la NetScaler VPX en 20.5.5.1 y se envía al usuario con la dirección IP 1.1.1.1.

- El cortafuegos VM-Series procesa todas las solicitudes entre los servidores de DMZ y el centro de datos corporativo. Para el contenido que reside en el centro de datos corporativo, el cortafuegos VM-Series procesa la solicitud de forma transparente (si se implementa usando las interfaces de capa 2 o de cable virtual) o la enruta (usando las interfaces de capa 3). Entonces, se facilita a la segunda instancia de la NetScaler VPX. Esta instancia de la NetScaler VPX equilibra las cargas de la solicitud en los servidores del centro de datos corporativo, dándole así servicio. El tráfico de retorno utiliza la misma ruta que la solicitud entrante.

  Por ejemplo, cuando un servidor de la DMZ (p. ej. 192.168.10.10) necesita contenido de un servidor del centro de datos corporativo (p. ej. 172.16.10.20), la dirección IP de destino es 172.168.10.3 (la VIP de la segunda NetScaler). La solicitud se envía al cortafuegos VM-Series en 192.168.10.2, donde el cortafuegos realiza una búsqueda de política y dirige la solicitud a 172.168.10.3. Entonces, la NetScaler VPX sustituye la dirección IP de destino, basada en el protocolo, por la dirección IP del servidor interno 172.16.10.20. El tráfico de retorno procedente de 172.168.10.20 se envía entonces a la NetScaler VPX en 172.168.10.3 y la dirección IP de origen se establece como 172.168.10.3 y se dirige al cortafuegos VM-Series en 172.168.10.2. En el cortafuegos VM-Series, se realiza de nuevo una búsqueda de política y el tráfico se dirige al servidor de la DMZ (192.168.10.10).

Para filtrar e informar sobre la actividad de los usuarios en la red, debido a que todas las solicitudes se inician desde la NetScaler VPX, debe activar la *inserción de encabezado* de HTTP o la *opción TCP para inserción de IP* en la primera instancia de la NetScaler VPX.

Configuración del cortafuegos VM-Series para asegurar el tráfico horizontal		
Paso 1	Instalación del Cortafuegos VM-Series en el servidor SDX	Si planea implementar el cortafuegos VM-Series usando interfaces de cable virtual o de capa 2, asegúrese de habilitar el modo de capa 2 en todas las interfaces de datos en el servidor de SDX.
Paso 2	Vuelva a conectar el cable a las interfaces asignadas a la NetScaler VPX.	Como la NetScaler VPX se reiniciará cuando vuelva a conectarse el cable, evalúe si desea realizar esta tarea durante una ventana de mantenimiento.
Paso 3	Configure las interfaces de datos.	Seleccione **Red > Interfaces** y asigne las interfaces como tipo de capa 3 (consulte el Paso 2), capa 2 (consulte el Paso 3) o cable virtual (consulte el Paso 3).
Paso 4	Cree la política de seguridad para permitir el tráfico de aplicación entre la DMZ y el centro de datos corporativo. Zona: De DMZ a Corporativa Observe que la regla de denegación implícita denegará todo el tráfico interno de la zona excepto el que permita explícitamente la política de seguridad.	1. Haga clic en **Añadir** en la sección **Políticas > Seguridad**. 2. Asigne a la regla un nombre descriptivo en la pestaña **General**. 3. En la ficha **Origen**, establezca la **zona de origen** como DMZ y la **dirección de origen** como 192.168.10.0/24. 4. En la ficha **Destino**, establezca la **zona de destino** como Corporativa y la **dirección de destino** como 172.168.10.0/24. 5. En la ficha **Aplicación**, seleccione las aplicaciones que desea permitir. Por ejemplo, Oracle. 6. Establezca **Servicio** como **Valor predeterminado de aplicación**. 7. En la pestaña **Acciones**, establezca **Configuración de acción** como Permitir. 8. Deje el resto de opciones con los valores predeterminados. 9. Haga clic en **Compilar** para guardar los cambios.

Para la protección del tráfico vertical, consulte Tráfico vertical seguro con el cortafuegos VM-Series.

Para obtener información general sobre las implementaciones, consulte Implementaciones compatibles: Cortafuegos VM Series en Citrix SDX.

Configuración del cortafuegos VM-Series edición NSX

El cortafuegos VM-Series edición NSX se ha desarrollado conjuntamente entre Palo Alto Networks y VMware. Esta solución emplea la API de NetX para integrar los cortafuegos de última generación de Palo Alto Networks y Panorama con los servidores ESXi de VMware para proporcionar una amplia visibilidad y una habilitación segura de aplicaciones de todo el tráfico de centros de datos, incluyendo comunicaciones con máquinas virtuales en el host.

Los siguientes temas ofrecen información sobre el cortafuegos VM-Series edición NSX.

- Presentación del cortafuegos VM-Series edición NSX
- Lista de comprobación de implementación del cortafuegos VM-Series edición NSX
- Creación de un grupo de dispositivos y plantillas en Panorama
- Registro del cortafuegos VM-Series como servicio en NSX Manager
- Implementación del cortafuegos VM-Series
- Creación de políticas
- Envío del tráfico desde los invitados que no ejecutan VMware Tools
- Grupos de direcciones dinámicas: Retransmisión de información desde NSX Manager a Panorama

Presentación del cortafuegos VM-Series edición NSX

NSX, la plataforma de redes y seguridad de VMware diseñada para el centro de datos definido por software (SDDC), ofrece la capacidad de implementar el cortafuegos de Palo Alto Networks como un servicio en un clúster de los servidores ESXi. El término *SDDC* es un término de VMware que hace referencia a un centro de datos en el que una infraestructura (recursos informáticos, red y almacenamiento) se virtualizan mediante NSX de VMware.

Para mantenerse al día con los cambios del ágil SDDC, la edición NSX del cortafuegos VM-Series simplifica el proceso de implementación de un cortafuegos de última generación de Palo Alto Networks y refuerza de forma continua la seguridad y conformidad normativa con el tráfico horizontal del SDDC. Si desea información detallada sobre VM-Series edición NSX, consulte los siguientes temas:

- ¿Cuáles son los componentes de la solución de la edición NSX?
- ¿Cómo se coordinan los componentes de la solución de la edición NSX?
- ¿Cuáles son las ventajas de la solución de la edición NSX?

¿Cuáles son los componentes de la solución de la edición NSX?

La Tabla: Componentes de VMware y la tabla Tabla: Componentes de Palo Alto Networks muestran los componentes de esta solución conjunta de Palo Alto Networks y VMware. En los siguientes temas se describe cada componente en profundidad:

- Servidor vCenter
- Administrador NSX
- Panorama
- VM-Series edición NSX
- Puertos/Protocolos usados en la comunicación de red

Tabla: Componentes de VMware

Componente	Descripción
Servidor vCenter	El servidor vCenter es la herramienta de gestión centralizada de la gama vSphere.
Administrador NSX	La plataforma Networking and Security de VMware debe instalarse y registrarse con el servidor vCenter. El administrador NSX es necesario para implementar el cortafuegos VM-Series edición NSX en los hosts ESXi dentro de un clúster ESXi.
Servidor ESXi	ESXi es un hipervisor que permite la virtualización informática.

Tabla: Componentes de Palo Alto Networks

Componente	Descripción
PAN-OS	La imagen base de VM-Series (PA-VM-NSX-6.1.1.zip) se usa para implementar el cortafuegos VM-Series edición NSX en PAN-OS 6.1. Los requisitos mínimos de sistema para implementar el cortafuegos VM-Series edición NSX en el servidor ESXi son los siguientes: • Dos vCPU, una para el plano de gestión y la otra para el plano de datos. Puede asignar 2 o 6 vCPU adicionales para asignar un total de 2, 4 u 8 vCPU al cortafuegos; el plano de gestión sólo usa una vCPU y puede asignar las vCPU adicionales al plano de datos. • 5 GB de memoria. Cualquier memoria adicional se utilizará únicamente en el plano de gestión. • 40 GB de espacio de disco virtual.

Componente	Descripción
Panorama Panorama debe estar ejecutando la misma versión o una versión más reciente que los cortafuegos que gestionará.	Panorama es la herramienta de gestión centralizada de los cortafuegos de última generación de Palo Alto Networks. En esta solución, Panorama trabaja con el administrador NSX para implementar, licenciar y administrar de forma centralizada (configuración y políticas) del cortafuegos VM-Series edición NSX. Panorama debe poder conectarse con el administrador NSX, el servidor vCenter, los cortafuegos VM-Series y el servidor de actualizaciones de Palo Alto Networks. Los requisitos mínimos de sistema de Panorama son los siguientes: • Dos vCPU de ocho núcleos (2,2 GHz); utilice 3 GHz si tiene 10 o más cortafuegos • 4 GB de RAM; se recomiendan 16 GB si tiene 10 cortafuegos o más • 40 GB de espacio en disco. Para ampliar la capacidad de registro, debe añadir un disco virtual o configurar el acceso a un almacén de datos NFS. Si desea información detallada, consulte la documentación de Panorama.
VM-Series edición NSX	La única licencia de VM disponible en esta solución es VM-1000 en modo de hipervisor (VM-1000-HV).

Tabla: Versiones compatibles

Componente	Versiones compatibles
Servidor vCenter	5.5
Servidor ESXi	5.5
Administrador NSX	• 6.0 con Panorama 6.0 y PAN-OS 6.0 Para implementar el cortafuegos VM-Series de la edición NSX con NSX Manager 6.0, consulte la Guía de implementación de VM-Series para la versión 6.0. • 6.1 con Panorama 6.1.1 y PAN-OS 6.0.x o 6.1.x (instrucciones en esta guía); la imagen base de NSX VM-Series sólo está disponible para PAN-OS 6.1.1 (no para 6.1.0). Para usar NSX Manager 6.1 con Panorama 6.0 y PAN-OS 6.0, debe usar la alternativa descrita en este artículo de base de conocimientos al usar las instrucciones de esta guía.

Servidor vCenter

El servidor vCenter es necesario para gestionar el administrador NSX y los hosts ESXi en su centro de datos. Esta solución conjunta requiere que los hosts ESXi se organicen en uno o más clústeres en el servidor vCenter y deben conectarse con un conmutador virtual distribuido.

Si desea información sobre clústeres, conmutadores virtuales distribuidos, DRS y el servidor vCenter, consulte su documentación de VMware: http://www.vmware.com/support/vcenter-server.html.

Administrador NSX

NSX es una plataforma de virtualización de red de VMware que se integra completamente con vSphere. El cortafuegos NSX y el compositor de servicios son funciones clave del administrador NSX. El cortafuegos NSX es un cortafuegos lógico que le permite vincular los servicios de redes y seguridad a las máquinas virtuales, y el compositor de servicios le permite agrupar máquinas virtuales y crear políticas para redirigir el tráfico al cortafuegos VM-Series (llamado servicio Palo Alto Networks NGFW en el administrador NSX).

Panorama

Panorama se usa para registrar la edición NSX del cortafuegos VM-Series como servicio *Palo Alto Networks NGFW* en el administrador NSX. El registro del servicio Palo Alto Networks NGFW en el administrador NSX permite a NSX Manager implementar la edición NSX del cortafuegos VM-Series en cada host ESXi del clúster ESXi.

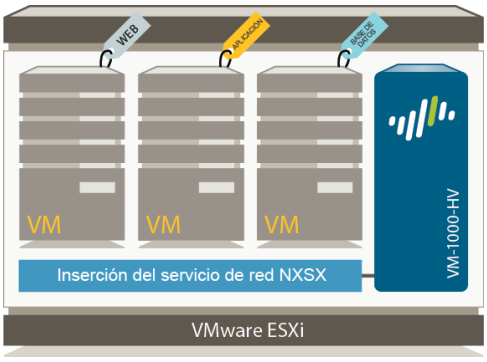
Panorama sirve como punto central de administración de los cortafuegos VM-Series edición NSX. Cuando se implementa un nuevo cortafuegos VM-Series edición NSX, se comunica con Panorama para obtener la licencia y recibe su configuración/políticas de Panorama. Todos los elementos de configuración, políticas y grupos de direcciones dinámicas de los cortafuegos gestionados pueden gestionarse de forma centralizada en Panorama mediante grupos de dispositivos y plantillas. La integración de la API XML basada en REST de esta solución permite a Panorama sincronizarse con el administrador NSX y los cortafuegos VM-Series edición NSX para permitir el uso de grupos de direcciones dinámicas y compartir el contexto entre el entorno virtualizado y la aplicación de seguridad. Para obtener más información, consulte Instauración de políticas mediante grupos de direcciones dinámicas.

VM-Series edición NSX

VM-Series edición NSX es el cortafuegos VM-Series que se implementa en el hipervisor ESXi. La integración con la API NetX posibilita automatizar el proceso de instalar el cortafuegos VM-Series directamente en el hipervisor ESXi y permite al hipervisor reenviar el tráfico al cortafuegos VM-Series sin usar la configuración vSwitch; por ello, no requiere ningún cambio a la topología de red virtual.

VM-Series edición NSX sólo admite interfaces cableadas virtuales. En esta edición Ethernet 1/1 y Ethernet 1/2 están vinculados mediante un cableado virtual y usa la API del plano de datos NetX para comunicarse con el hipervisor. Las interfaces de la capa 2 o la capa 3 no son obligatorias ni compatibles con VM-Series edición NSX, y por ello el cortafuegos no podrá realizar acciones de conmutación ni enrutamiento.

La única licencia disponible para esta versión del cortafuegos VM-Series es la VM-1000-HV. Si desea un breve resumen de la capacidad, consulte Modelos de VM-Series; si desea información completa sobre las capacidades máxima admitidas en la licencia VM-1000-HV, consulte la Hoja de datos de VM-Series.



Puertos/Protocolos usados en la comunicación de red

Para habilitar la comunicación de red necesaria para implementar el cortafuegos VMWare edición NSX, debe permitir el uso de los siguientes protocolos/puertos y aplicaciones.

- **Panorama**: Para obtener actualizaciones de software y actualizaciones dinámicas, Panorama usa SSL para acceder a updates.paloaltonetworks.com en TCP/443; esta URL utiliza la infraestructura CDN. Si necesita una única dirección IP, use staticupdates.paloaltonetworks.com. El AppID para actualizaciones es paloalto-updates.

  NSX Manager y Panorama usan SSL para comunicarse en TCP/443.

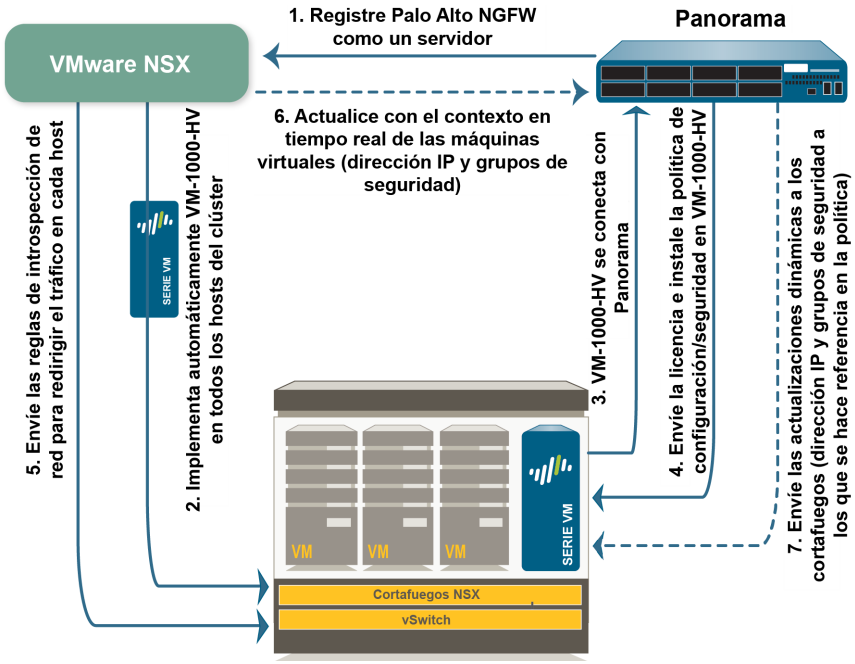
- **VM-Series edición NSX**: Si tiene pensado usar WildFire, los cortafuegos VM-Series deben tener acceso a wildfire.paloaltonetworks.com en el puerto 443. Se trata de una conexión SSL y el AppID es paloalto-wildfire-cloud.

  La interfaz de gestión en el cortafuegos VM-Series usa SSL para comunicarse con Panorama a través de TCP/3789.

- **Servidor vCenter**: El servidor vCenter debe ser capaz de alcanzar el servidor web de implementación que aloja el OVF VM-Series. El puerto es TCP/80 de manera predeterminada o navegación web de AppID.

¿Cómo se coordinan los componentes de la solución de la edición NSX?

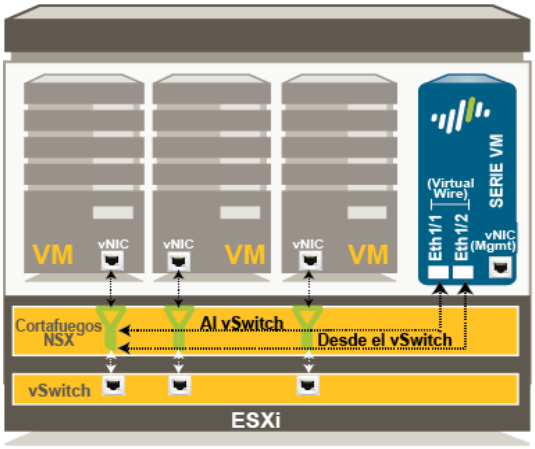
Para estar a la altura de los desafíos de seguridad del centro de datos definido por software, NSX Manager, los servidores ESXi y Panorama trabajan en perfecta sincronía para automatizar la implementación del cortafuegos VM-Series.



1. Registre el servicio Palo Alto Networks NGFW: El primer paso es registrar Palo Alto Networks NGFW como servicio en el administrador NSX. El proceso de registro usa la API del plano de gestión de NetX para activar la comunicación bidireccional entre Panorama y el administrador NSX. Panorama se configura con la dirección IP y las credenciales de acceso para iniciar la conexión y registrar el servicio Palo Alto Networks NGFW en el administrador NSX. La configuración incluye la URL de acceso de la imagen base de VM-Series que es obligatoria para implementar el cortafuegos VM-Series edición NSX, el código de autorización para recuperar la licencia y el grupo de dispositivos al que pertenecerán los cortafuegos VM-Series. NSX Manager usa esta conexión con el plano de gestión para compartir actualizaciones sobre los cambios en el entorno virtual con Panorama.

2. Implemente VM-Series automáticamente desde NSX: NSX Manager recopila la imagen base de VM-Series de la URL especificada durante el registro e instala una instancia del cortafuegos VM-Series en cada host ESXi del clúster ESXi. A partir de un grupo de IP de gestión estática (que define en NSX Manager), se asigna una dirección IP de gestión al cortafuegos VM-Series y la dirección IP de Panorama se proporciona al cortafuegos. Cuando el cortafuegos se inicia, la API de integración del plano de datos NetX conecta el cortafuegos VM-Series al hipervisor para que pueda recibir el tráfico desde el vSwitch.

Flujo de tráfico en la edición NSX de la serie VM



3. Establezca comunicación entre el cortafuegos VM-Series y Panorama: El cortafuegos VM-Series inicia una conexión con Panorama para obtener su licencia. Panorama recupera la licencia del servidor de actualización y la envía al cortafuegos. El cortafuegos VM-Series recibe la licencia (VM-1000-HV) y se reinicia con un número de serie válido.

4. Instale la configuración/política desde Panorama en el cortafuegos VM-Series: El cortafuegos VM-Series se vuelve a conectar con Panorama y proporciona su número de serie. Panorama ahora añade el cortafuegos al grupo de dispositivos que se definió en el proceso de registro y envía la política predeterminada al cortafuegos. El cortafuegos VM-Series ahora está disponible como máquina virtual de seguridad que puede configurarse más detalladamente para activar con seguridad las aplicaciones en la red.

5. Envío de las reglas de redireccionamiento de tráfico desde el cortafuegos NSX: En el compositor de servicios del cortafuegos NSX puede crear grupos de seguridad y definir reglas de introspección de red que especifiquen qué invitados de qué tráfico se enviarán al cortafuegos VM-Series. Consulte Reglas de políticas integradas para obtener información detallada.

Para garantizar que el tráfico de los invitados se envía al cortafuegos VM-Series, todos los invitados deben tener instalado VMware Tools. Si VMware Tools no está instalado, NSX Manager no conoce la dirección IP del invitado y, por lo tanto, el tráfico no se puede enviar al cortafuegos VM-Series. Para obtener más información, consulte Envío del tráfico desde los invitados que no ejecutan VMware Tools.

6. Reciba actualizaciones en tiempo real desde el administrador NSX: El administrador NSX envía actualizaciones en tiempo real de los cambios en el entorno virtual a Panorama. Estas actualizaciones incluyen información sobre los grupos de seguridad y direcciones IP de invitados que forman parte del grupo de seguridad cuyo tráfico se redirige al cortafuegos VM-Series. Consulte Reglas de políticas integradas para obtener información detallada.

7. Uso de grupos de direcciones dinámicas en actualizaciones dinámicas de envío y políticas desde Panorama a los cortafuegos VM-Series: En Panorama puede usar las actualizaciones en tiempo real de grupos de seguridad para crear grupos de direcciones dinámicas, vincularlas a políticas de seguridad y enviar esas políticas a los cortafuegos VM-Series. Todos los cortafuegos VM-Series del grupo de dispositivos tendrán el mismo conjunto de políticas, y ahora están completamente controlados para asegurar el SDDC. Consulte Instauración de políticas mediante grupos de direcciones dinámicas para obtener información detallada.

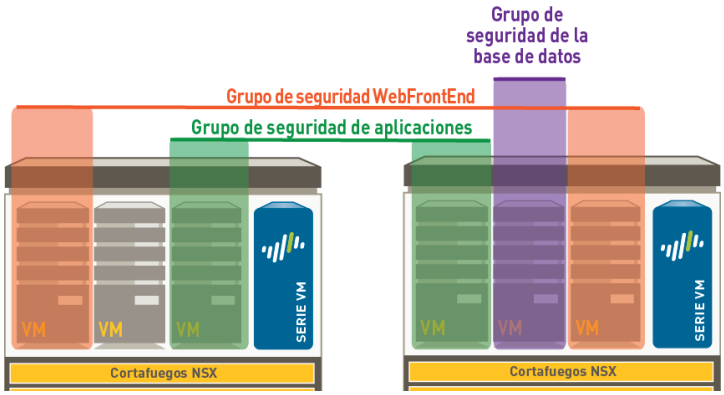
Reglas de políticas integradas

El cortafuegos NSX y el cortafuegos VM-Series colaboran para reforzar la seguridad; cada uno proporciona un conjunto de reglas de gestión de tráfico que se aplican al tráfico de cada host ESXi. El primer conjunto de reglas se define en el cortafuegos NSX; estas reglas determinan el tráfico desde el que se envían los invitados del clúster al cortafuegos VM-Series. El segundo conjunto de reglas (reglas de cortafuegos de próxima generación de Palo Alto Networks) se define en Panorama y se envía a los cortafuegos VM-Series. Estas son reglas de reforzamiento de seguridad para el tráfico que se envía al servicio Palo Alto Networks NGFW. Estas reglas determinan cómo debe procesar el cortafuegos VM-Series (admitir, denegar, inspeccionar y restringir) la aplicación para activarla con seguridad en su red.

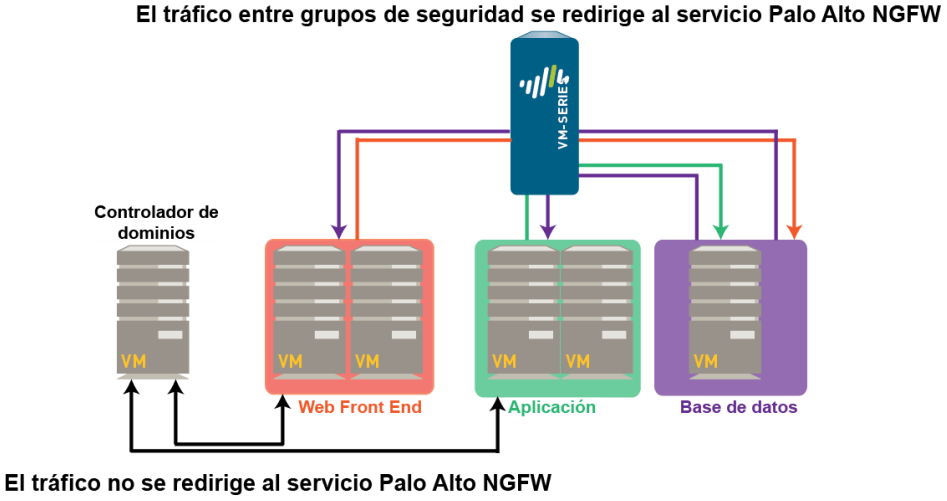
- **Reglas definidas en el cortafuegos NSX**: las reglas para dirigir el tráfico desde los invitados de cada host ESXi se configuran en el administrador NSX. El compositor de servicios en el administrador NSX le permite definir el tipo de protección de seguridad, como por ejemplo las reglas de cortafuegos que se aplicarán a los invitados del clúster ESXi. Para definir las reglas del cortafuegos NSX deberá agregar en primer lugar los invitados a grupos de seguridad y después crear políticas de composición del servicio NSX para redirigir el tráfico de estos grupos de seguridad al servicio Palo Alto Networks NGFW y el cortafuegos NSX.

  El siguiente diagrama ilustra la forma en que los grupos de seguridad pueden componerse de invitados en distintos hosts ESXi de un clúster.

Agrupación de invitados en grupos de seguridad de un clúster



  En el caso del tráfico que el cortafuegos VM-Series debe examinar y asegurar, las políticas del compositor de servicios NSX redirigen el tráfico al servicio Palo Alto Networks NGFW. Este tráfico se envía al cortafuegos VM-Series, que lo procesa antes de pasarlo al conmutador virtual.



El tráfico que el cortafuegos VM no tiene que inspeccionar, por ejemplo, la copia de seguridad de datos de red de ejemplo o el tráfico hacia un controlador de dominio interno, no tiene que redirigirse al cortafuegos VM-Series y puede enviarse al conmutador virtual para continuar su procesamiento.

- **Reglas gestionadas centralmente en Panorama y que aplica el cortafuegos VM-Series**: El cortafuegos VM-Series aplica reglas de cortafuegos de última generación. Estas reglas se definen y gestionan centralmente en Panorama mediante grupos de dispositivos y plantillas y se envían a los cortafuegos VM-Series. A continuación el cortafuegos VM-Series refuerza la política de seguridad comparando la dirección IP de origen o destino (el uso de grupos de direcciones dinámicas para cumplimentar los miembros del grupo en tiempo real y envía el tráfico a los filtros del cortafuegos NSX).

  Para entender la forma en que el administrador NSX y Panorama se sincronizan con los cambios en SDDC y garantizar que el cortafuegos VM-Series instaura constantemente la política, consulte Instauración de políticas mediante grupos de direcciones dinámicas.

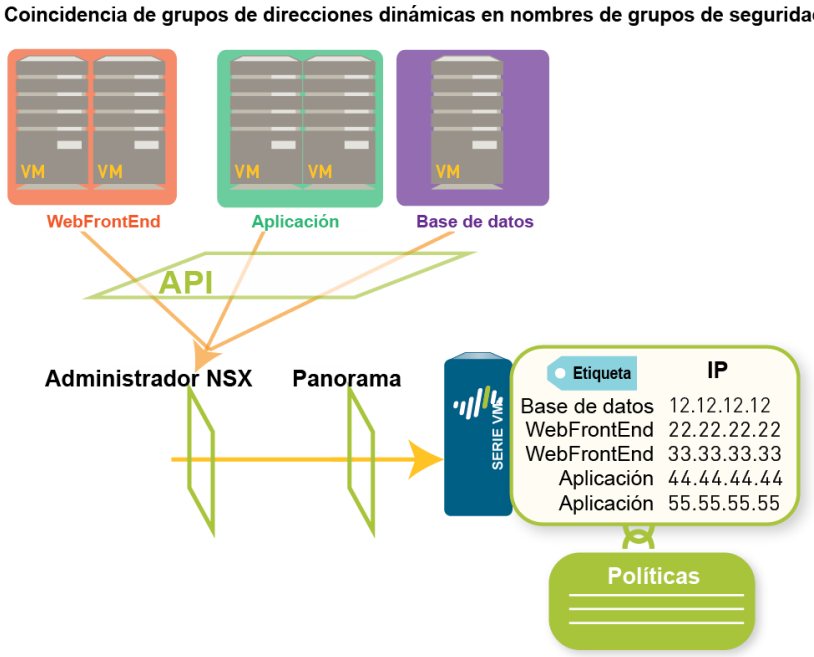
Instauración de políticas mediante grupos de direcciones dinámicas

A diferencia de otras versiones del cortafuegos VM-Series, la edición NSX no usa zonas de seguridad como mecanismo principal de segmentación del tráfico porque ambas interfaces de cableado virtual pertenecen a la misma zona. En su lugar, la edición NSX usa grupos de direcciones dinámicas para segmentar el tráfico.

Un grupo de direcciones dinámicas se usa como objeto de recurso o destino en una política de seguridad. Como las direcciones IP cambian constantemente en un entorno de centro de datos, los grupos de direcciones dinámicas ofrecen una forma de automatizar el proceso de referencia a las direcciones de origen o destino dentro de las políticas de seguridad. A diferencia de los objetos de direcciones estáticas, que deben actualizarse manualmente en la configuración y asignarse siempre que hay un cambio de dirección (adición, eliminación o traslado), los grupos de direcciones dinámicas se adaptan automáticamente a los cambios.

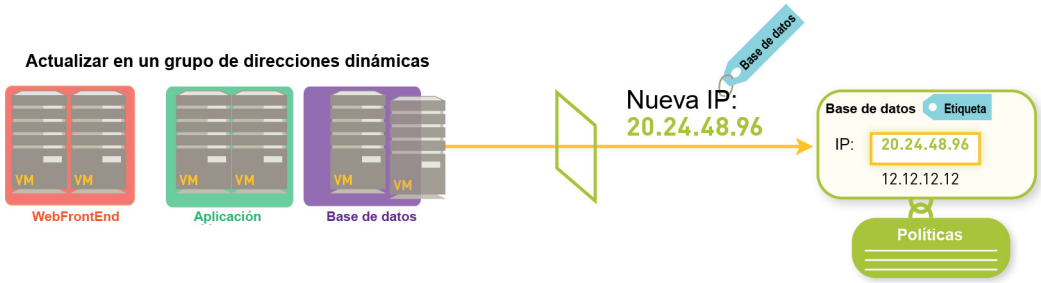
Todos los grupos de seguridad que se definen en NSX Manager se proporcionan automáticamente como actualizaciones de Panorama mediante la integración del plano de gestión de la API de NetX, y puede usarse como criterio de filtro para crear grupos de direcciones dinámicas; el cortafuegos filtra según el nombre del grupo de seguridad, que es una etiqueta, para encontrar todos los miembros que pertenecen a un grupo de seguridad.

Por ejemplo, si tiene una arquitectura multinivel para aplicaciones web, en el administrador NSX puede crear tres grupos de seguridad para los servidores WebFrontEnd, servidores de aplicaciones y servidores de bases de datos. El administrador NSX actualiza Panorama con el nombre de los grupos de seguridad y la dirección IP de los invitados que se incluyen en cada grupo de seguridad.



En Panorama puede crear tres grupos de direcciones dinámicas para los objetos etiquetados como de base de datos, aplicación y WebFrontEnd. A continuación, en la política de seguridad puede usar los grupos de direcciones dinámicas como objeto de origen o destino, definir las aplicaciones que pueden atravesar estos servidores y enviar las reglas a los cortafuegos VM.

Cada vez que se añade o modifica un invitado en el clúster ESXi o se actualiza o crea un grupo de seguridad, el administrador NSX usa la API XML basada en REST de PAN-OS para actualizar Panorama con la dirección IP y el grupo de seguridad al que pertenece el invitado. Para seguir el flujo de información, consulte Grupos de direcciones dinámicas: Retransmisión de información desde NSX Manager a Panorama.



Para asegurar que el nombre de cada grupo de seguridad es único, el servidor vCenter asigna una Id. de referencia de objeto gestionado (MOB) al nombre que defina para el grupo de seguridad. La sintaxis empleada para mostrar el nombre de un grupo de seguridad en Panorama es *nombre_especificado-securitygroup-número*; por ejemplo, *WebFrontEnd-securitygroup-47*.

Cuando Panorama recibe la notificación de la API verifica o actualiza la dirección IP de cada invitado y el grupo de seguridad al que pertenece ese invitado. A continuación Panorama envía esas actualizaciones en tiempo real a todos los cortafuegos que se incluyen en el grupo de dispositivos y notifica a los grupos de dispositivos de la configuración del gestor de servicios de Panorama.

En cada cortafuegos todas las reglas de políticas que hacen referencia a esos grupos de direcciones dinámicas se actualizan en el momento de la ejecución. Como el cortafuegos compara la etiqueta del grupo de seguridad para determinar los miembros de un grupo de direcciones dinámicas, no tiene que modificar ni actualizar la política cuando aplique cambios en el entorno virtual. El cortafuegos compara las etiquetas para buscar los miembros actuales de cada grupo de direcciones dinámicas y aplica la política de seguridad a la dirección IP de origen/destino que se incluye en el grupo.

¿Cuáles son las ventajas de la solución de la edición NSX?

La edición NSX del cortafuegos VM-Series se centra en asegurar las comunicaciones horizontales en el centro de datos definido por software. La implementación del cortafuegos tiene las siguientes ventajas:

- **Implementación automatizada**: el administrador NSX automatiza el proceso de distribución de los servicios de seguridad de cortafuegos de última generación y el cortafuegos VM permite una instauración transparente de la seguridad. Cuando se añade un host ESXi a un clúster, se implementa automáticamente un nuevo cortafuegos VM-Series, que se provisionen y está disponible para la instauración inmediata de políticas sin ninguna intervención manual. El flujo de trabajo automatizado le permite estar al día con las implementaciones de máquinas virtuales de su centro de datos. El modo de hipervisor del cortafuegos elimina la necesidad de reconfigurar los puertos/vSwitch/topología de red; como cada host ESXi tiene una instancia del cortafuegos, el tráfico no debe atravesar la red ni pasar por la red de retorno para su inspección y una instauración coherente de políticas.
- **Integración más estrecha entre el entorno virtual y la instauración de la seguridad dinámica**: los grupos de direcciones dinámicas están al día de los cambios en las máquinas/aplicaciones virtuales y garantizan que la política de seguridad está sincronizada con los cambios en la red. Esta capacidad de estar al día ofrece visibilidad y protección de las aplicaciones en un entorno ágil.
- **Gestión centralizada más sólida**: los cortafuegos implementados con esta solución se licencian y gestionan con Panorama, la herramienta de gestión centralizada de Palo Alto Networks. Si usa Panorama para gestionar los cortafuegos de centros de datos y perímetros (cortafuegos virtuales y basados en hardware), podrá centralizar la gestión de políticas y mantener la agilidad y coherencia en la instauración de políticas en toda la red.

En resumen, esta solución garantiza que la naturaleza dinámica de la red virtual se asegure con una carga administrativa mínima. Puede implementar con éxito aplicaciones con una mayor velocidad, eficiencia y seguridad.

Lista de comprobación de implementación del cortafuegos VM-Series edición NSX

Para implementar la edición NSX del cortafuegos VM-Series, debe usar el siguiente flujo de trabajo:

- **Paso 1: Configuración de componentes**: Para implementar VM-Series edición NSX, configure los siguientes componentes (consulte ¿Cuáles son los componentes de la solución de la edición NSX?:
  - Configure el servidor vCenter, instale y registre el administrador NSX con el servidor vCenter.

    Si aún no ha configurado el conmutador virtual y ha agrupado los hosts ESXi en los clústeres, consulte la documentación de VMware para ver instrucciones sobre la configuración del entorno vSphere. Este documento no le lleva por el proceso de configuración de los componentes VMware de esta solución.
  - Actualice Panorama a la versión 6.1.1. Creación de un grupo de dispositivos y plantillas en Panorama. Si no conoce Panorama, consulte la documentación de Panorama para ver instrucciones sobre la configuración de Panorama.
  - Descargue y guarde la plantilla ovf para la edición NSX del cortafuegos VM en un servidor web. NSX Manager debe tener acceso de red a este servidor web de modo que pueda implementar el cortafuegos VM-Series según sea necesario. No puede alojar la plantilla ovf en Panorama.
  - Registre el código de autenticación de capacidad del cortafuegos VM-Series de la edición NSX con su cuenta de asistencia técnica del portal de asistencia. Para obtener más información, consulte Aplique la licencia y actualice el Cortafuegos VM-Series.
- **Paso 2: Registro**: Configure Panorama en Registro del cortafuegos VM-Series como servicio en NSX Manager. Una vez registrado, el cortafuegos VM-Series se añade a la lista de servicios de red que NSX Manager puede implementar de forma transparente como servicio.

  También es necesaria una conexión entre Panorama y el administrador NSX para obtener licencia y configurar el cortafuegos.
- **Paso 3: Implemente los cortafuegos** y **cree políticas**: Instale el cortafuegos VM-Series y cree políticas para redirigir el tráfico al cortafuegos VM-Series y protegerlo. Consulte Implementación del cortafuegos VM-Series y Creación de políticas.
  - (En NSX Manager) Habilite SpoofGuard y defina reglas para bloquear protocolos no IP.
  - (En el administrador NSX) Defina el grupo de direcciones IP. Una dirección IP del rango definido se asigna a la interfaz de gestión de cada instancia del cortafuegos VM-Series.
  - (En NSX Manager) Implemente el cortafuegos VM-Series. El administrador NSX implementa automáticamente una instancia del VM-1000-HV en cada host ESXi del clúster.
  - (En NSX Manager) Configure los grupos de seguridad. Un grupo de seguridad reúne los invitados y aplicaciones especificados para que pueda aplicar la política al grupo. A continuación, cree las políticas del cortafuegos NSX para redirigir el tráfico al perfil de servicio de Palo Alto Networks.

NSX Manager usa la dirección IP como criterio de coincidencia para enviar el tráfico al cortafuegos VM-Series. Si VMware Tools no está instalado en el invitado, consulte Envío del tráfico desde los invitados que no ejecutan VMware Tools

- (En Panorama) Aplique políticas al cortafuegos VM-Series. En Panorama puede definir, enviar y administrar políticas centralmente en todos los cortafuegos VM-Series. En Panorama, cree grupos de acceso dinámico para cada grupo de seguridad y haga referencia a los grupos de acceso dinámico de la política; después, envíe las políticas a los cortafuegos gestionados.

  Este mecanismo de administración centralizada le permite asegurar los invitados y aplicaciones con una intervención administrativa mínima.

- **Paso 4: Supervisión y mantenimiento de la seguridad de red**: Panorama ofrece una completa vista gráfica del tráfico de la red. Utilizando las herramientas de visibilidad en Panorama [el Centro de comando de aplicación (ACC), logs y las funciones de generación de informes] puede analizar, investigar y elaborar informes de manera central sobre toda la actividad de red, identificar áreas con un posible impacto en la seguridad y traducirlas a políticas de activación de aplicaciones seguras. Si desea más información, consulte la Guía del administrador de Panorama.

Creación de un grupo de dispositivos y plantillas en Panorama

Para poder gestionar los cortafuegos de la edición NSX y VM-Series en Panorama, los cortafuegos deben pertenecer a un grupo de dispositivos; la adición de un cortafuegos a una plantilla es opcional. Los grupos de dispositivos le permiten reunir los cortafuegos que necesitan objetos y políticas similares como una unidad lógica; la configuración se define usando las fichas **Objetos** y **Políticas** en Panorama. Las plantillas se usan para configurar los ajustes necesarios para que los cortafuegos de la serie V operen en la red; la configuración se define usando las fichas **Dispositivo** y **Red** en Panorama. Por ejemplo, puede usar plantillas para definir un acceso administrativo al cortafuegos o definir ajustes de registro o perfiles de servidor en los cortafuegos gestionados.

Si no conoce Panorama, consulte la Guía del administrador de Panorama para ver instrucciones sobre la configuración de Panorama.

Creación de un grupo de dispositivos y plantillas en Panorama	
Paso 1 Inicie sesión en la interfaz web de Panorama.	Si usa una conexión segura (https) desde un navegador web, inicie sesión usando la dirección IP y la contraseña que asignó durante la configuración inicial. (`https://<dirección IP>`)
Paso 2 Añada un grupo de dispositivos.	1. Seleccione **Panorama > Grupos de dispositivos** y haga clic en **Añadir**. 2. Introduzca un **Nombre** y una **Descripción** exclusivos para identificar el grupo de dispositivos. 3. Haga clic en **ACEPTAR**. Cuando los cortafuegos se hayan implementado y abastecido, se mostrarán en **Panorama > Dispositivos gestionados** y se mostrará en el grupo de dispositivos. 4. Haga clic en **Compilar** y seleccione **Panorama** como **Compilar tipo** para guardar los cambios en la configuración que se esté ejecutando en Panorama.
Paso 3 (Opcional) Añada una plantilla.	1. Seleccione **Panorama > Plantillas** y haga clic en **Añadir**. 2. Introduzca un **Nombre** y una **Descripción** para identificar la plantilla Las opciones de **Modo de operación**, la casilla de verificación **Sistemas virtuales** y la casilla de verificación **Modo de deshabilitación de VPN** no se aplican al cortafuegos VM-Series. 3. Haga clic en **ACEPTAR**. 4. Haga clic en **Compilar** y seleccione **Panorama** como **Compilar tipo** para guardar los cambios en la configuración que se esté ejecutando en Panorama.

Registro del cortafuegos VM-Series como servicio en NSX Manager

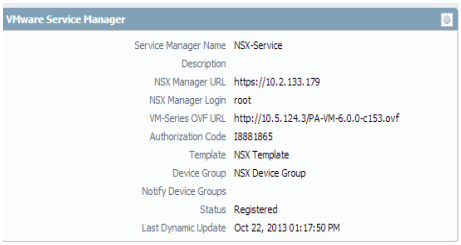
Para automatizar el abastecimiento del cortafuegos VM-Series edición NSX, habilite la comunicación entre NSX Manager y Panorama. Esta configuración se realiza una vez, y sólo debe modificarse si la dirección IP del NSX Manager cambia o se supera la licencia de capacidad de implementación del cortafuegos VM-Series.

Use Panorama para registrar el cortafuegos VM-Series como servicio		
Paso 1	Inicie sesión en la interfaz web de Panorama.	Use una conexión segura (https) desde un navegador web para iniciar sesión usando la dirección IP y la contraseña que asignó durante la configuración inicial (https://<*dirección IP*>).
Paso 2	Configure el acceso al administrador NSX.	1. Seleccione **Panorama > Administrador de servicios VMware**. 2. Introduzca el **Nombre de dominio del servidor**. En el administrador NSX este nombre aparece en la columna Administrador de servicios en **Redes y seguridad > Definiciones de servicio**. Consulte la captura de pantalla de Paso 9. 3. (Opcional) Añada una **Descripción** que identifique el cortafuegos VM-Series como servicio. 4. Introduzca la **URL de administrador NSX** (dirección IP o FQDN) a la que accederá NSX Manager. 5. Introduzca las credenciales de **Inicio de sesión del administrador NSX**; nombre de usuario y contraseña, de modo que Panorama pueda autenticarse en el NSX Manager.
Paso 3	Especifique la ubicación del archivo OVF. Extraiga y guarde los archivos .ovf y .vmdk en el mismo directorio. Estos archivos se usan para implementar cada instancia del cortafuegos. En caso necesario, modifique la configuración de seguridad para poder descargar los tipos de archivo. Por ejemplo, en el servidor IIS modifique la configuración Mime Types; en un servidor Apache, modifique el archivo .htaccess.	En **URL de OVF de VM-Series**, añada la ubicación del servidor web que aloja el archivo ovf. Tanto http como https son protocolos admitidos. Por ejemplo, introduzca **https://acme.com/software/PA-VM-NSX-6.1.1.ovf**

Use Panorama para registrar el cortafuegos VM-Series como servicio (Continuación)		
Paso 4	Adición del código de autorización. El código de autorización debe ser para el lote NSX del modelo VM-Series; por ejemplo, PAN-VM-1000-HV-PERP-BND-NSX Compruebe que la cantidad/capacidad del pedido es adecuada para admitir las necesidades de su red.	Introduzca el código de autorización que recibió con su correo electrónico de cumplimentación de pedidos. El código de autorización se usa para asignar una licencia a cada instancia de VM-Series. En el portal de asistencia técnica, puede visualizar el número total de cortafuegos que está autorizado a implementar y la proporción del número de licencias que se han usado del número total de licencias que le ofrece su código de autorización.
Paso 5	Especifique el grupo de dispositivos al que pertenecen los cortafuegos y, opcionalmente, la plantilla.	Como los cortafuegos implementados en esta solución se administran centralmente desde Panorama, debe especificar el **Grupo de dispositivos** al que pertenecen los cortafuegos. Todos los cortafuegos que se implementan con el código de autorización definido en el Paso 4 pertenecen a la plantilla y el grupo de dispositivos especificados durante la implementación inicial. Si quiere reasignar los cortafuegos, debe mover manualmente el cortafuegos a una plantilla o grupo de dispositivos distinto después de su implementación.
Paso 6	Configure la notificación en distintos grupos de dispositivos a medida que aprovisione nuevas máquinas virtuales o se produzcan cambios en la red.	Si desea que los entornos virtual y de seguridad estén al día para que las políticas se apliquen de forma coherente a todo el tráfico que se envía a los cortafuegos, deberá seleccionar el grupo de dispositivos al que hay que notificar. Seleccione los grupos de dispositivos aplicables en **Notificar grupos de dispositivos**. Los cortafuegos incluidos en los grupos de dispositivos especificados reciben una actualización en tiempo real de los grupos de dispositivos especificados reciben una actualización en tiempo real de grupos de seguridad y direcciones IP. Los cortafuegos usan esta actualización para determinar la lista más actual que constituye los grupos de direcciones dinámicas a los que se hace referencia en la política.
Paso 7	Compile los cambios realizados en Panorama.	Seleccione **Compilar** y Compilar tipo: **Panorama**.

Use Panorama para registrar el cortafuegos VM-Series como servicio (Continuación)

Paso 8 Verificación del estado de conexión en Panorama



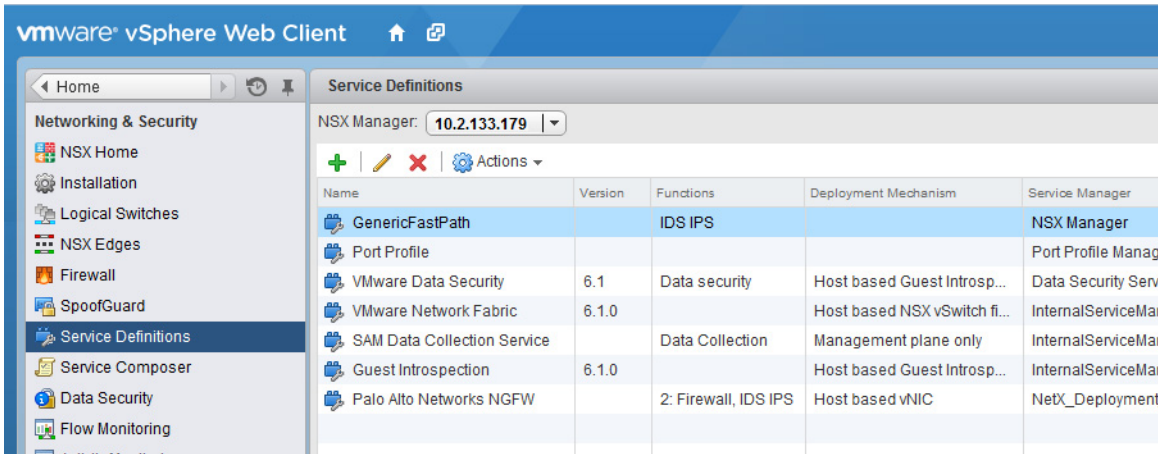
Muestra el estado de conexión entre Panorama y el administrador NSX. Cuando la conexión es correcta, el estado se muestra como **Registrado**. Esto indica que Panorama y NSX Manager están sincronizados y el cortafuegos VM-Series está registrado como servicio en NSX Manager.

Los mensajes de estados de error son:

- **No conectado**: No se ha podido alcanzar/establecer una conexión de red con el administrador NSX.
- **No autorizado**: Las credenciales de acceso (nombre de usuario y/o contraseña) son incorrectas.
- **No registrado**: El servicio, administrador del servicio o perfil del servicio no está disponible o se ha eliminado en el administrador NSX.
- **Sin sincronización**: Los ajustes de configuración definidos en panorama son distintos a lo que se ha definido en el administrador NSX.
- **Sin servicio/Sin perfil de servicio**: Indica una configuración incompleta en el administrador NSX.

Paso 9 Verifique que el cortafuegos se ha registrado como un servicio en NSX Manager.

1. En el cliente web de vSphere, seleccione **Redes y seguridad > Definiciones de servicio**.



2. Compruebe que **Palo Alto Networks NGFW** aparece en la lista de servicios disponibles para la instalación.

Implementación del cortafuegos VM-Series

Cuando haya registrado el cortafuegos VM-Series como un servicio (Palo Alto Networks NGFW) en NSX Manager, complete las siguientes tareas en NSX Manager.

- Habilite SpoofGuard
- Definición de un grupo de direcciones IP
- Preparación del host ESXi para el cortafuegos de VM-Series
- Implementación del servicio Palo Alto Networks NGFW

Habilite SpoofGuard

El cortafuegos distribuido de NSX sólo puede redirigir el tráfico al cortafuegos VM-series cuando hay una coincidencia con la dirección IP conocida para el servidor vCenter. Esto significa que cualquier tráfico L2 no IP, o tráfico IP que no coincida con las direcciones IP conocidas para el servidor vCenter, no coincidirá con las reglas de redireccionamiento definidas en NSX Manager y se desviará al cortafuegos VM-Series. Por lo tanto, para asegurarse de que todo el tráfico se filtre correctamente; deberá realizar los siguientes pasos.

- Habilite SpoofGuard para evitar el tráfico IP desconocido que de otro modo podría evitar el cortafuegos VM-series.

  Cuando SpoofGuard está habilitado, si la dirección IP de una máquina virtual cambia, el tráfico de la máquina virtual se bloqueará hasta que examine y apruebe el cambio de dirección IP en la interfaz de NSX SpoofGuard.

- Configure las reglas del cortafuegos NSX para bloquear el tráfico L2 no IP que no se pueda desviar al cortafuegos VM-Series.

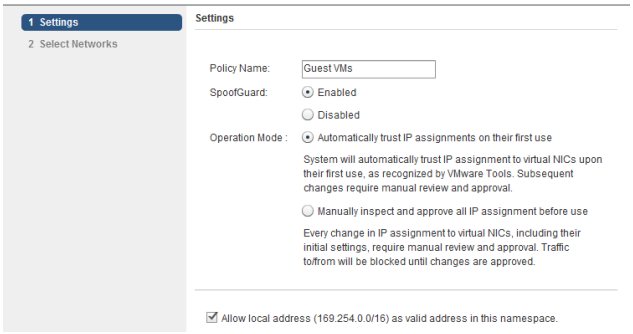
vCenter usa VMware Tools para conocer las direcciones IP de cada invitado. Si VMware Tools no está instalado en alguno de sus invitados, consulte Envío del tráfico desde los invitados que no ejecutan VMware Tools.

Habilite SpoofGuard y bloquee el tráfico L2 no IP

Paso 1 Habilite Spoofguard para los grupos de puertos que contienen los invitados.

Cuando esté habilitado, para cada adaptador de red, SpoofGuard inspecciona paquetes para la MAC preestablecida y su correspondiente dirección IP.

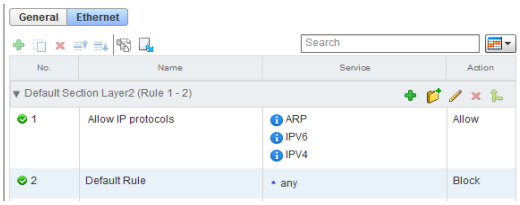
1. Seleccione **Redes y seguridad > SpoofGuard**.
2. Haga clic en **Añadir** para crear una nueva política y seleccione las siguientes opciones:
   - SpoofGuard: **Habilitado**
   - Modo de operación: **Confiar automáticamente en las asignaciones IP la primera vez que se usan**.
   - **Permitir direcciones locales como direcciones válidas en este espacio de nombre**.
   - Selección de redes: Seleccione los grupos de puertos a los que se conectan los invitados.



Habilite SpoofGuard y bloquee el tráfico L2 no IP (Continuación)

Paso 2 Seleccione los protocolos IP que se permitirán.

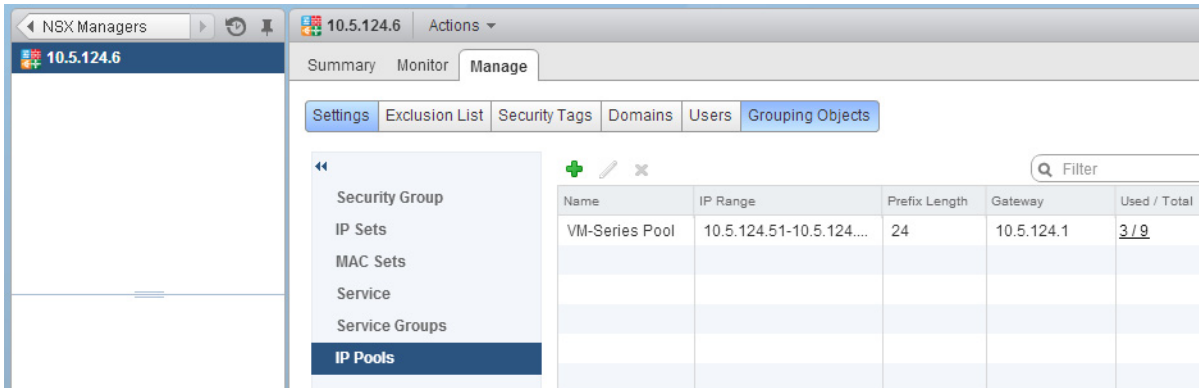
1. Seleccione **Redes y seguridad > Cortafuegos > Ethernet**.
2. **Añada** una regla que permita el tráfico **ARP**, **IPv4** e **IPv6**.
3. **Añada** una regla que bloquee todo lo demás.



Definición de un grupo de direcciones IP

El grupo de IP es un rango de direcciones IP (estáticas) que se reservan para establecer el acceso de gestión a los cortafuegos VM-Series. Cuando NSX Manager implementa un nuevo cortafuegos VM-Series, la primera dirección IP disponible de este rango se asigna a la interfaz de gestión del cortafuegos.

Definición de un grupo de direcciones IP	
Paso 1	En **Inventario de redes y seguridad,** seleccione **NSX Manager** y haga doble clic para abrir los detalles de configuración de NSX Manager.
Paso 2	Seleccione **Gestionar > Objetos de agrupación > Grupos de IP**.
Paso 3	Haga clic en **Añadir grupo de IP** y especifique los detalles de acceso de red solicitados en la pantalla que incluye el rango de direcciones IP estáticas que quiera usar para Palo Alto Networks NGFW.

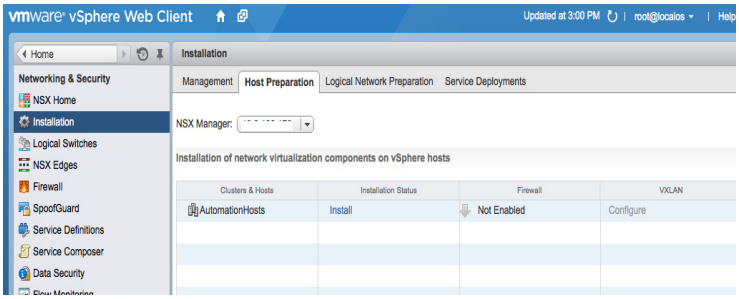


Preparación del host ESXi para el cortafuegos de VM-Series

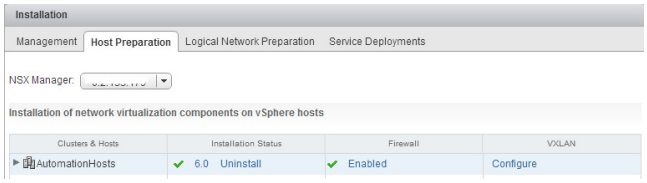
Antes de implementar el cortafuegos VM-Series, cada invitado del clúster debe tener los componentes de NSX necesarios que permitan que el cortafuegos NSX y el de VM-Series funcionen juntos. NSX Manager instalará los componentes (el módulo de adaptador de Ethernet (.eam) y el SDK) necesarios para implementar el cortafuegos VM-Series.

Preparación de los hosts ESXi para el cortafuegos VM-Series

1. En el administrador NSX, seleccione **Redes y seguridad > Instalación > Preparación del host**.

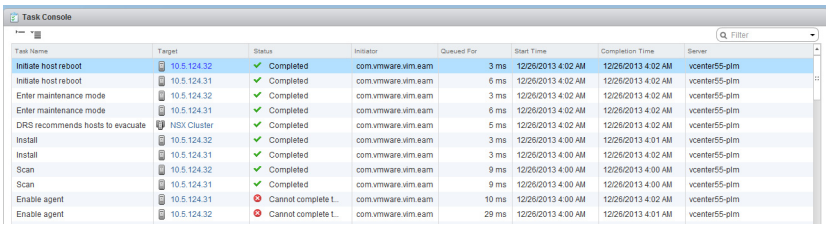


2. Haga clic en **Instalar** y verifique que el estado de instalación es correcto.



Este proceso se automatiza a medida que se añaden más hosts ESXi a un clúster, y los componentes NSX necesarios se instalan automáticamente en el host ESXi.

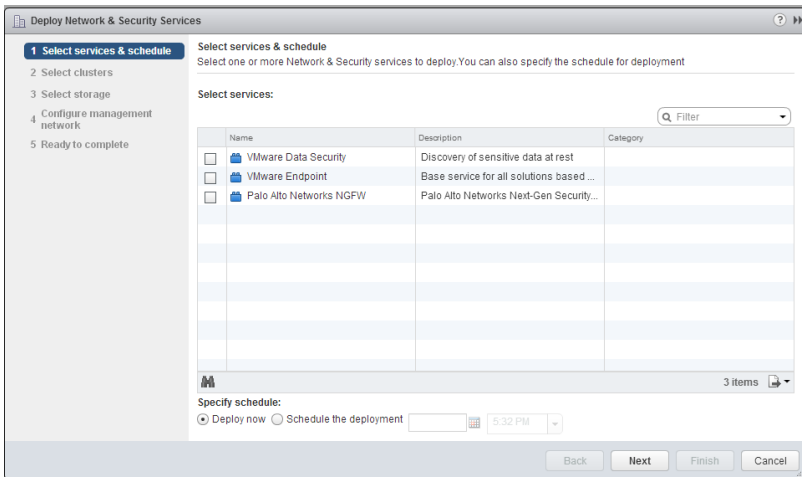
3. Si el estado de instalación no está listo o aparece una advertencia en la pantalla, haga clic en el vínculo **Resolver**. Para supervisar el progreso del intento de reinstalación, haga clic en el vínculo **Más tareas** y consulte que las siguientes tareas se hayan completado correctamente:



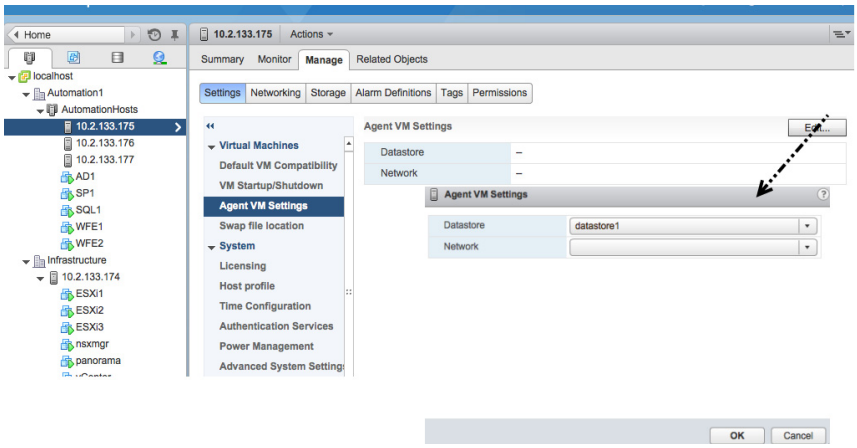
Implementación del servicio Palo Alto Networks NGFW

Realice los siguientes pasos para automatizar el proceso de implementación de una instancia del cortafuegos VM-Series edición NSX en cada host ESXi del clúster especificado.

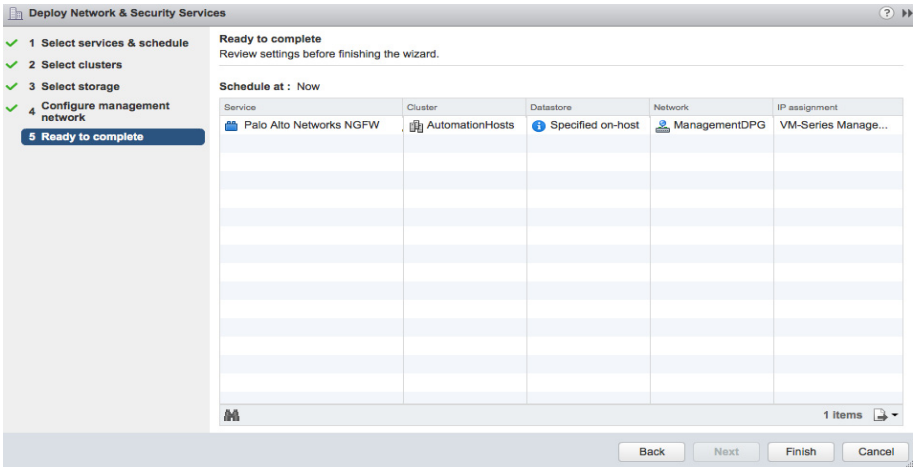
Implementación del servicio Palo Alto Networks NGFW	
Paso 1	Seleccione **Redes y seguridad > Instalación > Implementaciones de servicio**.
Paso 2	Haga clic en **Nueva implementación de servicio** (icono de signo más verde) y seleccione el servicio **Palo Alto Networks NGFW**. Haga clic en **Siguiente**.



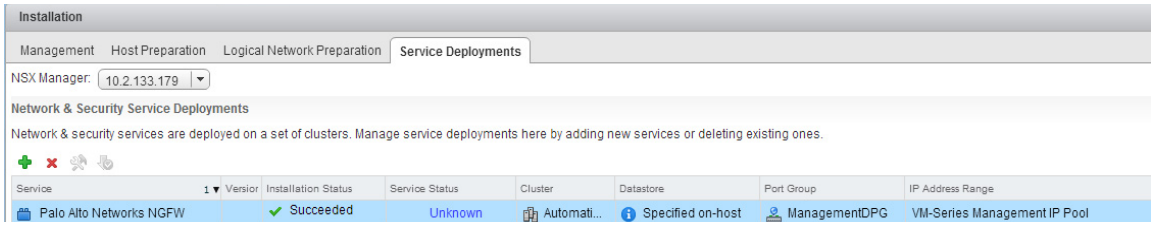
Paso 3	Seleccione el **Centro de datos** y los clústeres en los que se implementará el servicio. Una instancia del cortafuegos se implementará en cada host del clúster seleccionado.
Paso 4	Seleccione el almacén de datos en el que asignar espacio de disco para el cortafuegos. Seleccione una de las siguientes opciones según su implementación: • Si ha asignado un almacenamiento compartido al clúster, seleccione un almacén de datos compartido que esté disponible. • Si no ha asignado un almacenamiento compartido al clúster, seleccione la opción **Especificado en el host**. Asegúrese de seleccionar el almacenamiento cada host ESXi del clúster. Seleccione además la red que se usará para el tráfico de gestión en el cortafuegos VM-Series.



Implementación del servicio Palo Alto Networks NGFW (Continuación)	
Paso 5	Seleccione el grupo de puertos que proporciona acceso de tráfico de red de gestión al cortafuegos.
Paso 6	Seleccione el grupo de direcciones IP (que definió en Definición de un grupo de direcciones IP) desde el que asignar una dirección IP de gestión a cada cortafuegos cuando se implementa.
Paso 7	Revise la configuración y haga clic en **Finalizar**.

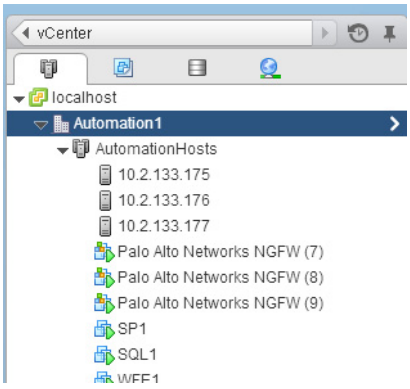


Paso 8	Compruebe que el administrador NSX comunica que el **Estado de instalación** es **Correcto**. Este proceso puede tardar un tiempo, haga clic en el vínculo **Más tareas** en vCenter para supervisar el progreso de la instalación.



Si la instalación de VM-Series falla, el mensaje de error se mostrará en la columna Estado de instalación. También puede usar la ficha **Tareas** y el **Explorador de registros** en el administrador NSX para ver los detalles del fallo y consultar la documentación de VMware para conocer los pasos de resolución de problemas.

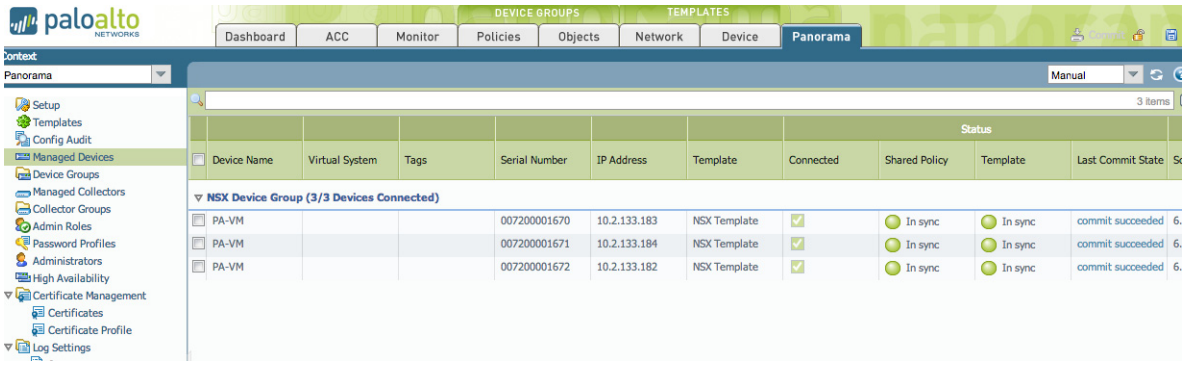
Paso 9	Compruebe que el cortafuegos se ha implementado con éxito y está conectado a Panorama. En el servidor vCenter, seleccione **Hosts y clústeres** para comprobar que todos los hosts del clúster tienen una instancia del cortafuegos.



Implementación del servicio Palo Alto Networks NGFW (Continuación)

Paso 10 Acceda a la interfaz web de Panorama para asegurarse de que los cortafuegos VM-Series están conectados y sincronizados con Panorama.

1. Seleccione **Panorama > Dispositivos gestionados** para comprobar que los cortafuegos están conectados y sincronizados.

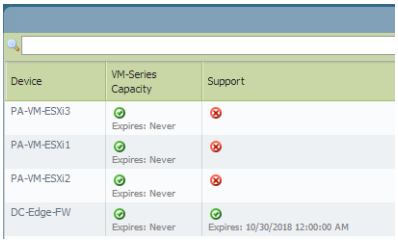


2. Haga clic en **Compilar** y seleccione Compilar tipo como **Panorama**.

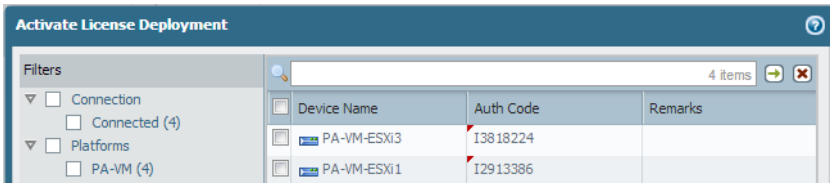
Es necesario compilar Panorama periódicamente para garantizar que Panorama guarda los números de serie de dispositivos en la configuración. Si reinicia Panorama sin compilar los cambios, los dispositivos gestionados no se conectarán de nuevo con Panorama; aunque el grupo de dispositivos aparecerá en la lista de dispositivos, los dispositivos no aparecerán en **Panorama > Dispositivos gestionados**.

Paso 11 Compruebe que se ha aplicado la licencia de capacidad y cualquier licencia adicional que haya adquirido. Como mínimo debe activar la licencia de asistencia técnica en cada cortafuegos.

1. Seleccione **Panorama > Implementaciones de servicio > Licencias** para comprobar que la licencia de capacidad de VM-Series se aplique.



2. Para aplicar licencias adicionales a los cortafuegos VM-Series:
   - Haga clic en **Activar** en **Panorama > Implementación de dispositivos > Licencias**.
   - Busque o filtre el cortafuegos y, en la columna **Código de autenticación**, introduzca el código de autorización de la licencia a activar. Solo es posible introducir un código de autorización una vez para cada cortafuegos



3. Haga clic en **Activar** y compruebe que la activación de la licencia se realizó con éxito.

Paso 12 (Opcional) Actualice la versión de PAN-OS en los cortafuegos VM-Series, consulte Actualización de la versión de software de PAN-OS (edición NSX).

Creación de políticas

Los siguientes temas describen cómo crear políticas en NSX Manager para redirigir el tráfico al cortafuegos VM-Series y cómo crear políticas en Panorama y aplicarlas en el cortafuegos VM-Series para que este pueda instaurar la política en el tráfico que se le redirige.

▲ Definición de políticas en el administrador NSX

▲ Aplicación de políticas al cortafuegos de VM-Series

Definición de políticas en el administrador NSX

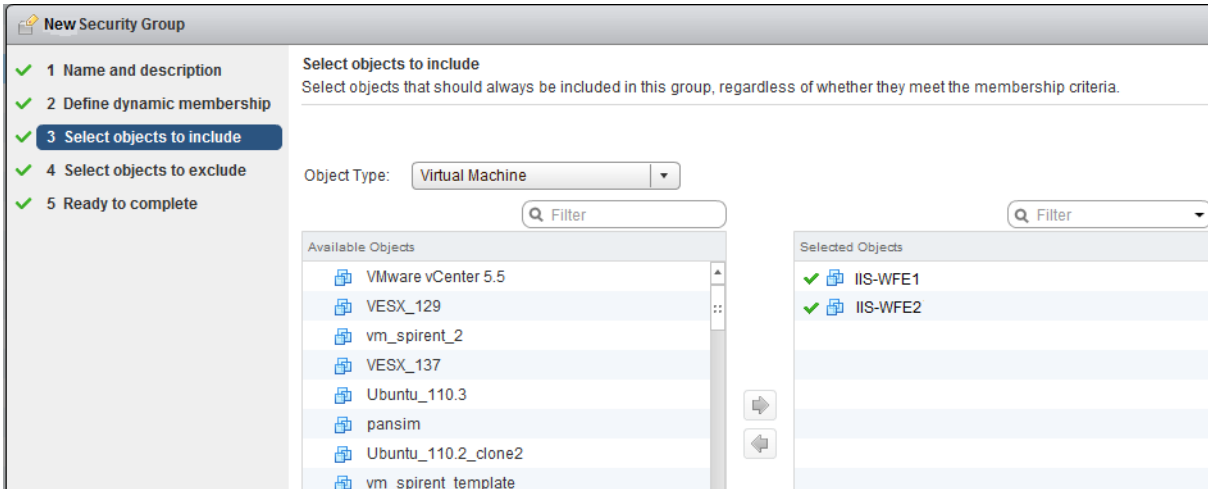
Para que el cortafuegos VM-Series proteja el tráfico, debe completar las siguientes tareas:

- Configuración de grupos de seguridad en NSX Manager
- Redirija el tráfico al cortafuegos VM-Series
- Aplicación de políticas al cortafuegos de VM-Series.

Configuración de grupos de seguridad en NSX Manager

Un grupo de seguridad es un contenedor lógico que reúne invitados en múltiples hosts ESXi del clúster. La creación de los grupos de seguridad facilita la gestión de los invitados y su seguridad; para comprender cómo los grupos de seguridad permiten la instauración de políticas, consulte Instauración de políticas mediante grupos de direcciones dinámicas.

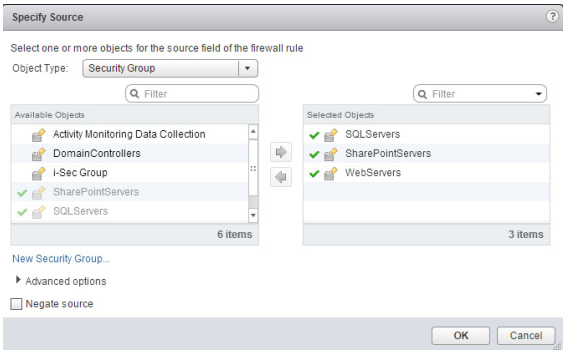
Configuración de grupos de seguridad en NSX Manager	
Paso 1	Seleccione **Redes y seguridad > Compositor de servicios > Grupos de seguridad** y agregue un **Nuevo grupo de seguridad**.
Paso 2	Añada un **nombre** y una **descripción**. Este nombre aparecerá en la lista de criterios de coincidencia cuando defina los grupos de direcciones dinámicas en Panorama.
Paso 3	Seleccione los invitados que constituyen el grupo de seguridad. Puede añadir miembros dinámica o estáticamente. Puede **definir la pertenencia dinámica** mediante la coincidencia de etiquetas de seguridad (recomendado) **seleccionar los objetos que se incluirán** de manera estática. En la siguiente captura de pantalla, los invitados que pertenecen al grupo de seguridad se seleccionan usando la opción **Tipo de objeto**: **Máquina virtual**.



Paso 4	Revise la información y haga clic en **Aceptar** para crear el grupo de seguridad.

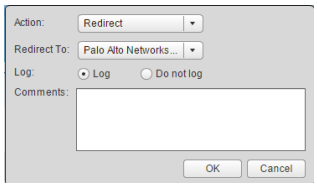
Redirija el tráfico al cortafuegos VM-Series

No aplique las políticas de redireccionamiento de tráfico a no ser que comprenda el funcionamiento de las reglas en NSX Manager, así como en el cortafuegos VM-Series y Panorama. La política predeterminada en el cortafuegos VM-Series se define como *denegar todo* el tráfico, lo que significa que todo el tráfico que se redirija al cortafuegos VM-Series será descartado. Para crear políticas en Panorama y enviarlas al cortafuegos VM-Series, consulte Aplicación de políticas al cortafuegos de VM-Series.

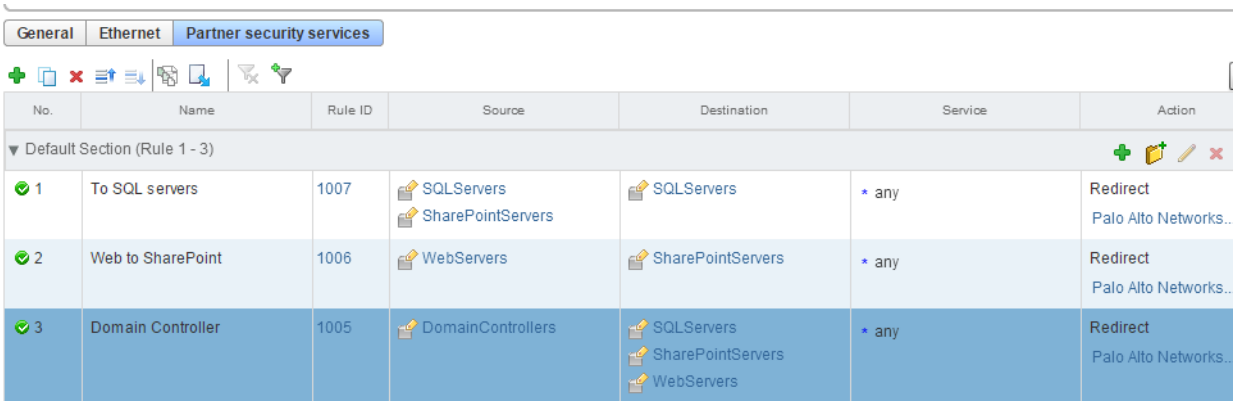
Definición de las reglas del cortafuegos NSX para redirigir el tráfico al cortafuegos VM-Series	
Paso 1	Seleccione **Redes y seguridad > Cortafuegos > Configuración** y haga clic en **Servicios de seguridad de socios**.
Paso 2	En la columna Acción, haga clic en el icono verde con el símbolo más y añada una regla de **nombre**.
Paso 3	Especifique el **origen** desde el que se redirigirá el tráfico. En el menú desplegable **Tipo de objeto**, seleccione **Grupo de seguridad** y seleccione uno de los grupos que definió anteriormente. Haga clic en **ACEPTAR**. 
Paso 4	Especifique el **destino** del flujo del tráfico. En el menú desplegable **Tipo de objeto**, seleccione **Grupo de seguridad** y seleccione el grupo relevante. Haga clic en **ACEPTAR**.

Definición de las reglas del cortafuegos NSX para redirigir el tráfico al cortafuegos VM-Series (Continuación)

Paso 5 Especifique la **acción** para el tráfico. Redirija el tráfico al perfil de servicio de Palo Alto Networks que creó anteriormente; **Palo Alto Networks perfil 1** en este flujo de trabajo**.** Este perfil especifica las redes/grupos de puertos/grupos de seguridad desde los que el cortafuegos recibe tráfico de datos.

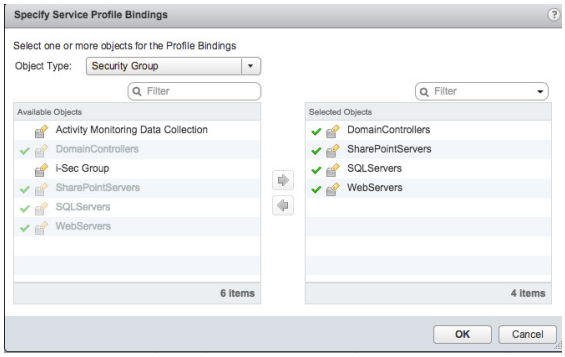


Si, por ejemplo, desea inspeccionar todo el tráfico entrante desde los grupos de seguridad a los servidores front-end web y todo el tráfico saliente de los servidores a los grupos de seguridad, la regla sería como sigue:



Paso 6 Vincule uno o más grupos de seguridad o grupos de puertos distribuidos o conmutadores lógicos al perfil de servicio de Palo Alto Networks. No puede mezclar y hacer coincidir los tipos de objetos. El tráfico de cada host ESXi incluido en su selección se redirigirá al cortafuegos.

1. En la columna **Acción** de las reglas del cortafuegos que acaba de crear, haga clic en el enlace **Palo Alto Networks perfil 1**.
2. Seleccione el **Tipo de objeto** y uno o más objetos que quiera vincular al perfil, y haga clic en **ACEPTAR**.



3. **Publique** sus cambios.

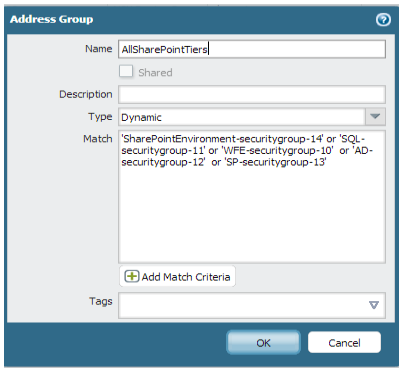
Aplicación de políticas al cortafuegos de VM-Series

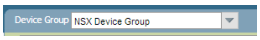
Ahora que ha creado las políticas de seguridad en el administrador NSX, los nombres de los grupos de seguridad a los que se hace referencia en la política de seguridad estarán disponibles en Panorama. Ahora puede usar Panorama para administrar centralmente políticas en los cortafuegos VM-Series.

Para gestionar una política centralizada, primero debe crear un grupo de direcciones dinámicas que coincida con el nombre de los grupos de direcciones dinámicas que coincidan con los grupos de seguridad que defina en el administrador NSX. Después, adjuntará el grupo de direcciones dinámicas como una dirección de origen o destino en la política de seguridad y lo enviará a los cortafuegos; los cortafuegos puede recuperar dinámicamente las direcciones IP de las máquinas virtuales que se incluyen en cada grupo de seguridad para garantizar que el tráfico que se origina o se dirige a las máquinas virtuales del grupo especificado cumple los requisitos.

Definición de políticas en Panorama

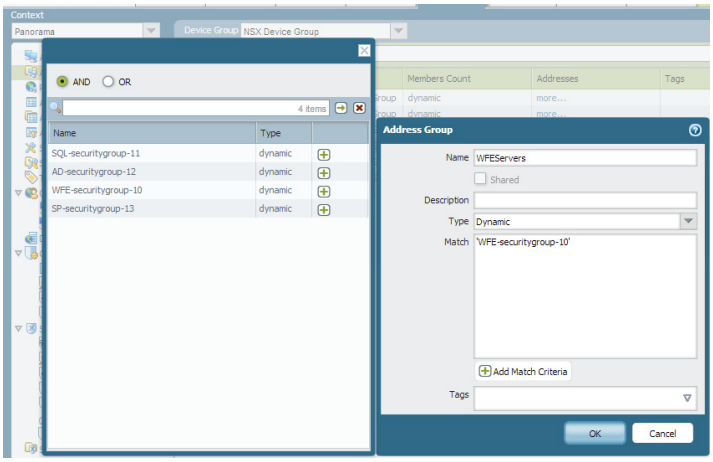
Paso 1 Creación de grupos de direcciones dinámicas.



1. Inicie sesión en la interfaz web de Panorama.
2. Seleccione **Objeto > Grupos de direcciones**.
3. Seleccione el **Grupo de dispositivos** 

que creó para gestionar los cortafuegos VM-Series edición NSX en Creación de un grupo de dispositivos y plantillas en Panorama.
4. Haga clic en **Añadir** e introduzca un **Nombre** y una **Descripción** del grupo de direcciones.
5. Defina el **Tipo** como **Dinámico**.
6. Haga clic en **Añadir criterios de coincidencia**. Seleccione el operador **Y** u **O** y seleccione ⊕ junto al nombre del grupo de seguridad que desea comparar.

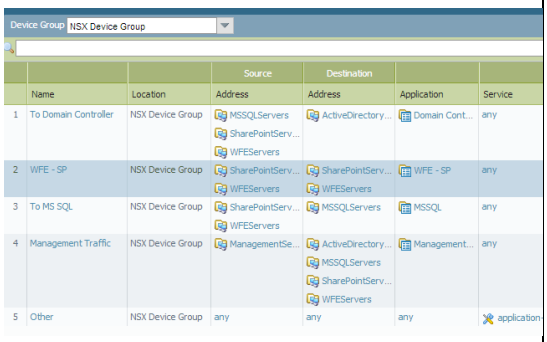
   Los grupos de seguridad que aparecen en los criterios de coincidencia derivan de los grupos que definió en el compositor de servicios en NSX Manager. Aquí sólo están disponibles los grupos de seguridad a los que se hace referencia en las políticas de seguridad y desde los que se redirige el tráfico al cortafuegos VM-Series.

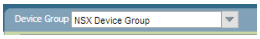


7. Haga clic en **ACEPTAR**.
8. Repita los pasos 4-7 para crear el número adecuado de Grupos de direcciones dinámicas para su red.
9. Haga clic en **Compilar**.

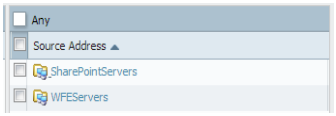
Definición de políticas en Panorama (Continuación)

Paso 2 Cree políticas de seguridad.

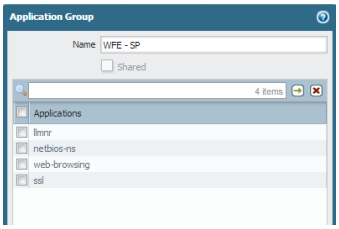


1. Seleccione **Políticas > Seguridad**.
2. Seleccione el **Grupo de dispositivos** 

que creó para gestionar los cortafuegos VM-Series edición NSX en Creación de un grupo de dispositivos y plantillas en Panorama.
3. Haga clic en **Añadir** e introduzca un **Nombre** y una **Descripción** para la regla. En este ejemplo la regla de seguridad permite todo el tráfico entre los servidores WebFrontEnd y de aplicaciones.
4. En **Dirección de origen** y **Dirección de destino**, seleccione o escriba una dirección, grupo de direcciones o región. En este ejemplo, seleccionamos un grupo de direcciones, el grupo de direcciones dinámico que creó en el Paso 1 anterior.

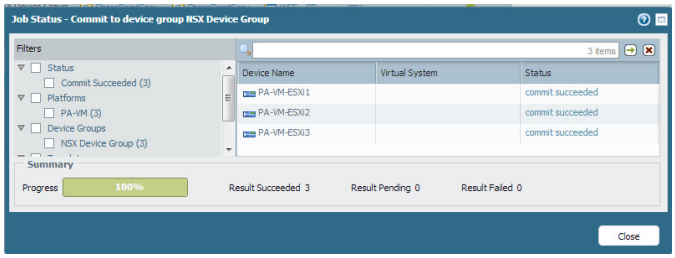
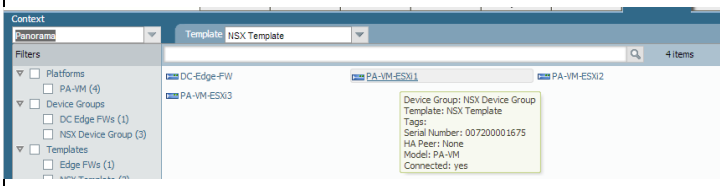
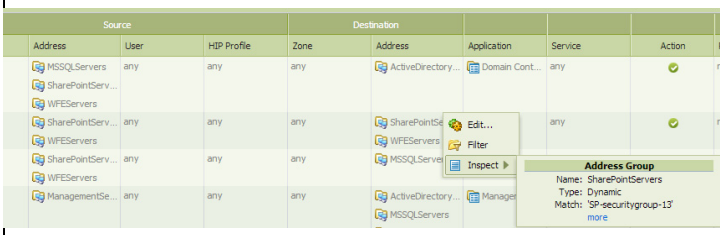
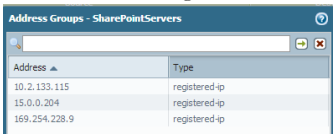


5. Seleccione la **Aplicación** a permitir. En este ejemplo hemos creado un **Grupo de aplicaciones** que incluye un grupo estático de aplicaciones específicas que se agrupan juntas.
   a. Haga clic en **Añadir** y seleccione **Nuevo grupo de aplicaciones**.
   b. Haga clic en **Añadir** para seleccionar la aplicación que desea añadir al grupo. En este ejemplo seleccionamos lo siguiente:
   c. Haga clic en **ACEPTAR** para crear el grupo de aplicaciones.



6. Especifique la acción (**Permitir** o **Denegar**) para el tráfico y, opcionalmente, adjunte los perfiles de seguridad predeterminados para los antivirus, anti-spyware y protección contra vulnerabilidades en **Perfiles.**
7. Repita los pasos 3- 6 anterior para crear las reglas de políticas pertinentes.
8. Haga clic en **Compilar** y seleccione Compilar tipo como **Panorama**. Haga clic en **ACEPTAR**.

Definición de políticas en Panorama (Continuación)

Paso 3 Aplique las políticas a los cortafuegos VM-Series edición NSX.	1. Haga clic en **Compilar** y seleccione Compilar tipo como **Grupos de dispositivos**. 2. Seleccione el grupo de dispositivos, que en este ejemplo es Grupo de dispositivos NSX, y haga clic en **Aceptar**. 3. Verifique que la compilación se realiza correctamente. 
Paso 4 Valide que los miembros del grupo de direcciones dinámicas se cumplimentan en el cortafuegos VM-Series. No puede verificar los miembros (direcciones IP registradas) del grupo de direcciones dinámicas en Panorama. Esta información sólo puede verse en el cortafuegos VM-Series que instaura la política.	1. En Panorama, cambie el contexto del dispositivo para iniciar la interfaz web del cortafuegos al que envió las políticas.  2. En el cortafuegos VM-Series, seleccione **Políticas > Seguridad** y seleccione una regla. 3. Seleccione la flecha desplegable junto al vínculo del grupo de direcciones y seleccione **Inspeccionar**. También puede comprobar si los criterios de coincidencia son precisos.  4. Haga clic en el vínculo **más** y compruebe que se muestra la lista de direcciones IP registradas.  La política entra en vigor para todas las direcciones IP que pertenecen a este grupo de direcciones y se muestra aquí.
Paso 5 (Opcional) Use la plantilla para enviar una configuración base para la configuración de red y dispositivo, como por ejemplo servidor DNS, servidor NTP, servidor Syslog y pancarta de inicio de sesión.	Si desea más información sobre el uso de plantillas, consulte la Guía del administrador de Panorama.

Envío del tráfico desde los invitados que no ejecutan VMware Tools

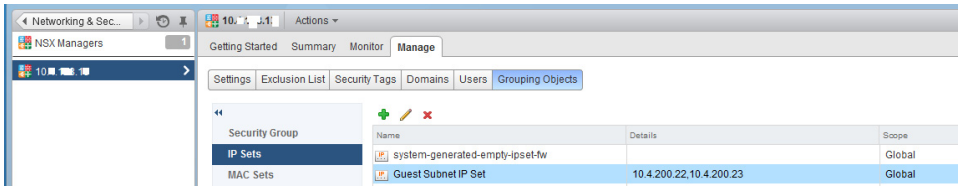
VMware Tools contiene una utilidad que permite a NSX Manager recopilar las direcciones IP de cada invitado que se ejecuta en el clúster. NSX Manager usa la dirección IP como criterio de coincidencia para enviar el tráfico al cortafuegos VM-Series. Si no tiene VMware Tools instalado en todos los invitados, las direcciones IP del invitado no están disponibles para NSX Manager y el tráfico no se puede enviar al cortafuegos VM-Series.

Los siguientes pasos le permiten aprovisionar invitados sin VMware Tools para que el tráfico de estos invitados pueda ser gestionado por el cortafuegos VM-Series.

Envío del tráfico desde los invitados que no ejecutan VMware Tools

Paso 1 Cree un grupo de IP que incluya a los invitados que necesiten protección del cortafuegos VM-Series. Este grupo de IP se usará como objeto de origen o destino en una regla de cortafuegos distribuido NSX en el Paso 4 a continuación.

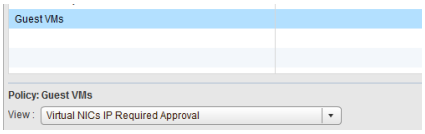
1. Seleccione **NSX Managers > Gestionar > Objetos de agrupación > Grupos de IP**.
2. Haga clic en **Añadir** e introduzca la dirección IP de cada invitado que no tiene VMware Tools instalado y necesita ser protegido por el cortafuegos VM-Series. Use comas para separar direcciones IP individuales; no se admiten subredes o intervalos de IP.



Paso 2 Verifique que SpoofGuard está habilitado. Si no lo está, consulte Habilite SpoofGuard.

Paso 3 Apruebe manualmente las direcciones IP para cada invitado en SpoofGuard; de este modo valida que las direcciones IP son las correctas para el adaptador de red. Para una dirección IP configurada manualmente, asegúrese de añadir la dirección IP al grupo de IP antes de aprobarla en SpoofGuard.

1. Seleccione la nueva política de SpoofGuard que ha creado anteriormente y **vea: Tarjetas de red virtuales inactivas**.
2. Seleccione el invitado y añada la dirección IP en el campo IP aprobada y publique los cambios.
3. Consulte y apruebe también todas las direcciones IP aprobadas previamente.



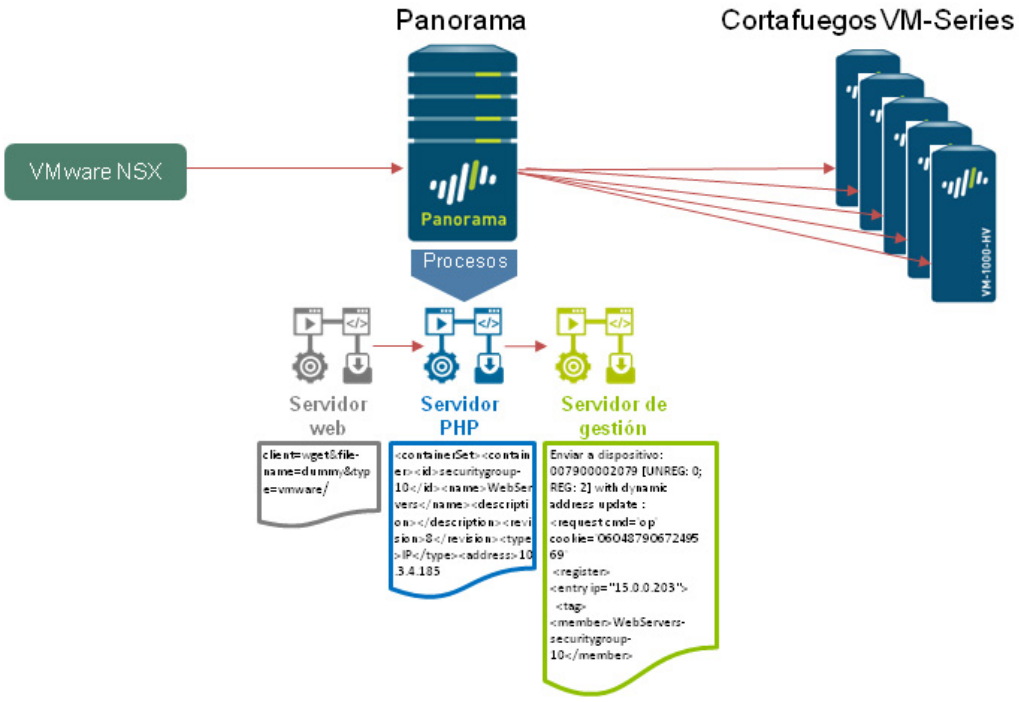
Paso 4 Añada los grupos de IP a Grupos de seguridad en NSX para forzar la política.

1. Seleccione **Redes y seguridad > Compositor de servicios > Grupos de seguridad.**
2. Seleccione **Seleccionar objetos para incluir > Grupos de IP**; añada el grupo de objetos de IP que se incluirá.

Grupos de direcciones dinámicas: Retransmisión de información desde NSX Manager a Panorama

Para forzar políticas de seguridad en un centro de datos integrado en VM-Series y NSX, Panorama debe poder obtener la información de los cambios en el entorno virtual. Conforme se implementan, cambian o eliminan nuevas máquinas virtuales, NSX Manager informa a Panorama de las direcciones IP añadidas, eliminadas de los grupos de seguridad en NSX Manager. Panorama envía a su vez esta información a los cortafuegos VM-Series. Los grupos de direcciones dinámicas incluidos en las políticas de cortafuegos buscan coincidencias con esta información para determinar los miembros que pertenecen al grupo. Este proceso permite al cortafuegos forzar una política de seguridad compatible con el contexto, lo que protege el tráfico hacia y desde estas máquinas virtuales. Para ver información sobre grupos de direcciones dinámicas, consulte Instauración de políticas mediante grupos de direcciones dinámicas.

El siguiente diagrama ilustra el modo en que la información se retransmite desde NSX Manager a Panorama.



Para comprender este proceso, sigamos la actualización de información enviada desde NSX Manager a Panorama cuando se añade un nuevo servidor a un grupo de seguridad. Use los elementos resaltados en los resultados de cada fase de este ejemplo para resolver el problema en el punto donde se produce.

Flujo desde el NSX Manager a Panorama		
Paso 1	Para ver las actualizaciones en tiempo real, inicie sesión en la CLI de Panorama.	Inicie sesión en la interfaz de línea de comando de Panorama.

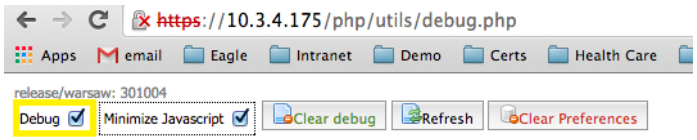
Flujo desde el NSX Manager a Panorama (Continuación)	

Paso 2 Compruebe que la solicitud desde NSX Manager se enruta al servidor web en Panorama.	Para comprobar el log del servidor web en Panorama durante una actualización del grupo de seguridad de NSX, use el siguiente comando:
	`admin@Panorama> **tail follow yes webserver-log cmsaccess.log**`
	`127.0.0.1 - - [Wed Dec 03 14:24:11 2014 PST] "POST /unauth/php/RestApiAuthenticator.php HTTP/1.1" 200 433`
	`127.0.0.1 - - [Wed Dec 03 14:24:11 2014 PST] "PUT /api/index.php?client=wget&file-name=dummy&type=vmware/vmware/2.0/si/serviceprofile/serviceprofile-1/containerset HTTP/1.0" 200 446`
	Si el resultado no incluye los elementos anteriores, compruebe si hay problemas con el enrutamiento. Haga ping a Panorama desde NSX Manager y compruebe si hay ACL u otros dispositivos de seguridad de red que puedan estar bloqueando la comunicación entre NSX Manager y Panorama.

Flujo desde el NSX Manager a Panorama (Continuación)

Paso 3 Compruebe que el daemon PHP en Panorama procesa la solicitud.

1. Habilite la depuración mediante la siguiente URL: `https://<Panorama_IP>/php/debug/utils/debug.php`



2. Desde la CLI, introduzca el siguiente comando para ver los logs generados por el servidor PHP:

```
admin@Panorama> tail follow yes mp-log
php.debug.log
[2014/12/03 14:24:11]
<request cmd="op" cookie="0604879067249569"
refresh="no">
  <operations xml="yes">
    <show>
      <cli>
...
   <request>
      <partner>
        <vmware-service-manager>
          <update>
            <method>PUT</method>
            <type>update</type>
            <username>_vsm_admin</username>
             <password>4006474760514053</password>
<url>/vmware/2.0/si/serviceprofile/serviceprofil
e-1/containerset</url>
            <data><![CDATA[
<containerSet><container><id>securitygroup-10</i
d><name>WebServers</name><description></descript
ion><revision>8</revision><type>IP</type><addres
s>10.3.4.185</address><address>10.3.4.186</addre
ss><address>15.0.0.203</address><address>15.0.0.
202</address></container></containerSet>]]></dat
a>
          </update>
        </vmware-service-manager>
      </partner>
    </request>
  </operations>
</request>
```

Flujo desde el NSX Manager a Panorama (Continuación)

Paso 4 El servidor de gestión en Panorama procesa la información.	1. Habilite la depuración en el servidor de gestión mediante el comando siguiente:
	`admin@Panorama> debug management-server on debug`
	2. Introduzca el siguiente comando para ver los logs generados por el log configd:
	`admin@Panorama> tail follow yes mp-log configd.log`
	3. En los resultados, compruebe que la actualización se ha retransmitido desde el daemon PHP al daemon del servidor de gestión.
	`2014-12-03 14:24:11.143 -0800 debug: pan_job_progress_monitor(pan_job_mgr.c:3694): job-monitor: updated 0 jobs`
	`.....`
	`2014-12-03 14:24:11.641 -0800 debug: recursive_add_params(pan_op_ctxt.c:158): > 'url'='/vmware/2.0/si/serviceprofile/serviceprofile-1/containerset'`
	`2014-12-03 14:24:11.641 -0800 debug: recursive_add_params(pan_op_ctxt.c:158): > 'data'='`
	`<containerSet><container><id>securitygroup-10</id><name>WebServers</name><description></description><revision>8</revision><type>IP</type><address>10.3.4.185</address><address>10.3.4.186</address><address>15.0.0.203</address><address>15.0.0.202</address></container></containerSet>'`
	`2014-12-03 14:24:11.641 -0800 Received vshield update: PUT /vmware/2.0/si/serviceprofile/serviceprofile-1/containerset`
	`Received dynamic address update from VSM:`
	`<request cmd='op' cookie='0604879067249569' client="xmlapi"><operations xml='yes'><request>`
	`<partner>`
	`<vmware-service-manager>`
	`<update>`
	`<method>PUT</method>`
	`<type>update</type>`
	`<username>_vsm_admin</username>`
	`<password>4006474760514053</password>`
	`<url>/vmware/2.0/si/serviceprofile/serviceprofile-1/containerset</url>`
	`<data><![CDATA[`
	`<containerSet><container><id>securitygroup-10</id><name>WebServers</name><description></description><revision>8</revision><type>IP</type><address>10.3.4.185</address><address>10.3.4.186</address><address>15.0.0.203</address><address>15.0.0.202</address></container></containerSet>]]>`
	`</data>`
	`</update>`

Flujo desde el NSX Manager a Panorama (Continuación)	
	4. Busque la lista de direcciones IP y las etiquetas de los grupos de seguridad. 2014-12-03 14:24:11.646 -0800 debug: pan_cfg_mongo_sel_ip_taglist_by_tag_rev(src_cms/pan_cfg_mongo_tables.c:3721): **ip: 10.3.4.185** 2014-12-03 14:24:11.646 -0800 debug: pan_cfg_mongo_sel_ip_taglist_by_tag_rev(src_cms/pan_cfg_mongo_tables.c:3738): **tag: WebServers-securitygroup-10** 2014-12-03 14:24:11.646 -0800 debug: pan_cfg_mongo_sel_ip_taglist_by_tag_rev(src_cms/pan_cfg_mongo_tables.c:3721): **ip: 15.0.0.202** 2014-12-03 14:24:11.646 -0800 debug: pan_cfg_mongo_sel_ip_taglist_by_tag_rev(src_cms/pan_cfg_mongo_tables.c:3738): **tag: WebServers-securitygroup-10** pan_cfg_mongo_sel_ip_taglist_by_tag_rev(src_cms/pan_cfg_mongo_tables.c:3738): **tag: DomainControllers-securitygroup-16** 2014-12-03 14:24:11.647 -0800 debug: pan_cfg_mongo_sel_ip_taglist_by_tag_rev(src_cms/pan_cfg_mongo_tables.c:3721): **ip: 15.0.0.201** 2014-12-03 14:24:11.648 -0800 debug: pan_cfg_mongo_sel_ip_taglist_by_tag_rev(src_cms/pan_cfg_mongo_tables.c:3738): **tag: SQLServers-securitygroup-11** 2014-12-03 14:24:11.665 -0800 debug: pan_cfg_mongo_sel_ip_taglist_by_tag_rev(src_cms/pan_cfg_mongo_tables.c:3738): **tag: SharePointServers-securitygroup-13** 2014-12-03 14:24:11.665 -0800 debug: pan_cfg_mongo_sel_ip_taglist_by_tag_rev(src_cms/pan_cfg_mongo_tables.c:3721): **ip: 10.3.4.187** 2014-12-03 14:24:11.665 -0800 debug: pan_cfg_mongo_sel_ip_taglist_by_tag_rev(src_cms/pan_cfg_mongo_tables.c:3738): **tag: SharePointServers-securitygroup-13** ...

Flujo desde el NSX Manager a Panorama (Continuación)	

	5. Por último, compruebe que la actualización se ha retransmitido desde el daemon del servidor de gestión a los cortafuegos gestionados.
	`Send to device: 007900002079 [UNREG: 0; REG: 2] with dynamic address update :`
	`<request cmd='op' cookie='0604879067249569' target-`
	`….`
	`<register>`
	`<entry ip="15.0.0.203">`
	`<tag>`
	`<member>WebServers-securitygroup-10</member>`
	`</tag>`
	`</entry>`
	`<entry ip="10.3.4.186">`
	`<tag>`
	`<member>WebServers-securitygroup-10</member>`
	`</tag>`
	`</entry>`
	`</register>`

Si se completa este proceso, los cortafuegos pueden forzar la política y proteger estos servidores correctamente.

Configuración del cortafuegos VM-Series en AWS

El cortafuegos VM-Series puede implementarse en la nube de Amazon Web Services (AWS): Se puede configurar para proteger el acceso a las aplicaciones implementadas en instancias de EC2 en una Virtual Private Cloud (VPC) en AWS.

- Acerca del cortafuegos VM-Series en AWS
- Implementaciones compatibles con AWS
- Implementación del cortafuegos VM-Series en AWS
- Caso de uso: Protección de las instancias de EC2 en AWS Cloud
- Caso de uso: Uso de grupos de direcciones dinámicas para proteger las nuevas instancias de EC2 en la VPC
- Caso de uso: Cortafuegos VM-Series como puertas de enlace de GlobalProtect en AWS
- Lista de atributos supervisados en la VPC de AWS

Acerca del cortafuegos VM-Series en AWS

Amazon Web Services (AWS) es un servicio de nube pública que le permite ejecutar sus aplicaciones en una infraestructura compartida gestionada por Amazon. Estas aplicaciones se pueden implementar en capacidades de procesamiento de tamaño variable o en instancias de EC2 en diferentes regiones de AWS y a las que los usuarios pueden acceder a través de Internet. Para ofrecer una conectividad de red consistente e instancias de EC2 fáciles de gestionar, Amazon ofrece Virtual Private Cloud (VPC). Una VPC se distribuye desde la nube pública de AWS y se asigna a un bloque CIDR desde el espacio de red privada (RFC 1918). Dentro de una VPC, puede crear subredes públicas o privadas según sus necesidades e implementar las aplicaciones en instancias de EC2 dentro de esas subredes. A continuación, para permitir el acceso a las aplicaciones dentro de la VPC, puede implementar el cortafuegos de VM-Series en una instancia de EC2. El cortafuegos de VM-Series se puede configurar para proteger el tráfico desde y hacia las instancias de EC2 dentro de la VPC.

En este documento se da por hecho que ya conoce la red y la configuración de la VPC de AWS. Con el fin de proporcionar contexto para los términos utilizados en esta sección, a continuación presentamos una breve actualización sobre los términos de AWS (algunas definiciones se han tomado directamente del glosario de AWS) a los que se hace referencia en este documento:

Término	Descripción
EC2	Elastic Compute Cloud Un servicio web que le permite iniciar y gestionar instancias de servidores Linux/UNIX y Windows en centros de datos de Amazon.
AMI	Amazon Machine Image Una AMI proporciona la información necesaria para iniciar una instancia, que es un servidor virtual en la nube. La AMI de VM-Series es una imagen de equipo cifrada que incluye el sistema operativo necesario para crear una instancia del cortafuegos de VM-Series en una instancia de EC2.
Tipo de instancia	Las especificaciones definidas por Amazon que determinan la memoria, CPU, capacidad de almacenamiento y coste por hora de una instancia. Algunos tipos de instancias están diseñados para aplicaciones estándar, mientras que otros están diseñados para aplicaciones de uso intensivo de la memoria y la CPU, etc.
ENI	Interfaz de red elástica Una interfaz de red adicional que se puede adjuntar a una instancia EC2. Las ENI pueden incluir una dirección IP privada principal, una o más direcciones IP privadas secundarias, una dirección IP pública, una dirección IP elástica (opcional), una dirección MAC, miembros de grupos de seguridad especificados, una descripción y una marca de comprobación de origen/destino.

Término	Descripción
Tipos de direcciones IP para instancias de EC2	Una instancia de EC2 puede tener diferentes tipos de direcciones IP. • Dirección IP pública: Una dirección IP que se puede enrutar a través de Internet. • Dirección IP privada: Una dirección IP en el intervalo de direcciones IP privadas como se define en RFC 1918. Puede elegir asignar manualmente una dirección IP o asignar automáticamente una dirección IP dentro del intervalo en el bloque CIDR para la subred en la que inicia la instancia de EC2. Si asigna manualmente direcciones IP, Amazon reserva las primeras cuatro (4) direcciones IP y la última dirección IP en cada subred para el uso de redes IP. • Dirección IP elástica (EIP): Una dirección IP estática que ha asignado en Amazon EC2 o Amazon VPC y, a continuación, adjuntado a una instancia. Las direcciones IP elásticas están asociadas a su cuenta, no a una instancia específica. Son elásticas porque se pueden asignar, adjuntar, desasociar y liberar fácilmente en función de sus necesidades. Una instancia en una subred pública puede tener una dirección IP privada, una dirección IP pública y una dirección IP elástica (EIP); una instancia en una subred pública tendrá una dirección IP privada y, de manera opcional, una EIP.
VPC	Virtual Private Cloud Una red elástica que incluye infraestructura, plataforma y servicios de aplicaciones que comparten una seguridad e interconexión comunes.
IGW	Puerta de enlace de Internet ofrecida por Amazon. Conecta una red a Internet. Puede enrutar el tráfico de las direcciones IP fuera de su VPC a la puerta de enlace de Internet.
Subredes	Un segmento del intervalo de direcciones IP de una VPC a la que se pueden adjuntar instancias de EC2. Las instancias de EC2 se agrupan en subredes en función de sus necesidades de seguridad y operativas. Hay dos tipos de subredes: • Subred privada: No se puede acceder a las instancias de EC2 en esta subred desde Internet. • Subred pública: La puerta de enlace de Internet está adjuntada a la subred pública, y se puede acceder a las instancias de EC2 en esta subred desde Internet.
Grupos de seguridad	Un grupo de seguridad se adjunta a una ENI y especifica la lista de protocolos, puertos e intervalos de direcciones IP que tienen permiso para establecer conexiones entrantes y salientes en la interfaz. En la VPC de AWS, los grupos de seguridad y las ACL de red controlan el tráfico entrante y saliente; los grupos de seguridad regulan el acceso a la instancia de EC2, mientras que las ACL de red regulan el acceso a la subred. Dado que está implementando el cortafuegos VM-Series, establezca reglas más permisivas en sus grupos de seguridad y ACL de red y permita al cortafuegos habilitar aplicaciones de forma segura en la VPC.
Tablas de enrutamiento	Un conjunto de reglas de enrutamiento que controla el tráfico saliente de cualquier subred asociada a una tabla de enrutamiento. Una subred puede estar asociada a una sola tabla de enrutamiento.

Término	Descripción
Par de claves	Un conjunto de credenciales de seguridad que puede usar para demostrar su identidad de manera electrónica. El par de claves consiste en una clave privada y una pública. En el momento de iniciar el cortafuegos VM-Series, debe generar un par de claves o seleccionar uno existente para el cortafuegos VM-Series. La clave privada es obligatoria para acceder al cortafuegos en el modo de mantenimiento.

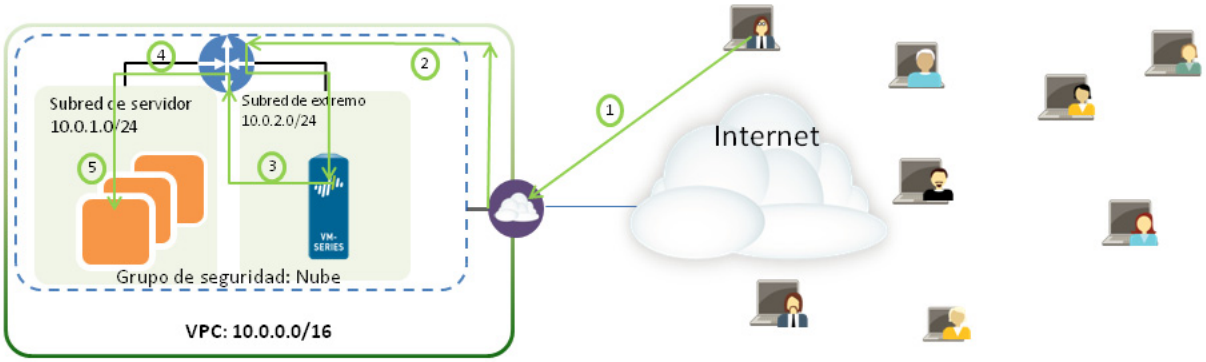
Implementaciones compatibles con AWS

El cortafuegos VM-Series protege el tráfico entrante y saliente de las instancias de EC2 dentro de la Virtual Private Cloud (VPC) de AWS. Dado que la VPC de AWS sólo admite una red IP (funciones de red de capa 3), el cortafuegos VM-Series sólo se puede implementar con interfaces de capa 3.

- Implemente el cortafuegos VM-Series para proteger las instancias de EC2 alojadas en la AWS Virtual Private Cloud.

  Si aloja sus aplicaciones en la nube de AWS, implemente el cortafuegos VM-Series para proteger y habilitar de forma segura aplicaciones para los usuarios que acceden a las mismas a través de Internet. Por ejemplo, el siguiente diagrama muestra el cortafuegos VM-Series implementado en la subred de extremo a la que está adjuntada la puerta de enlace. Las aplicaciones se implementan en la subred privada, que no tiene acceso directo a Internet.

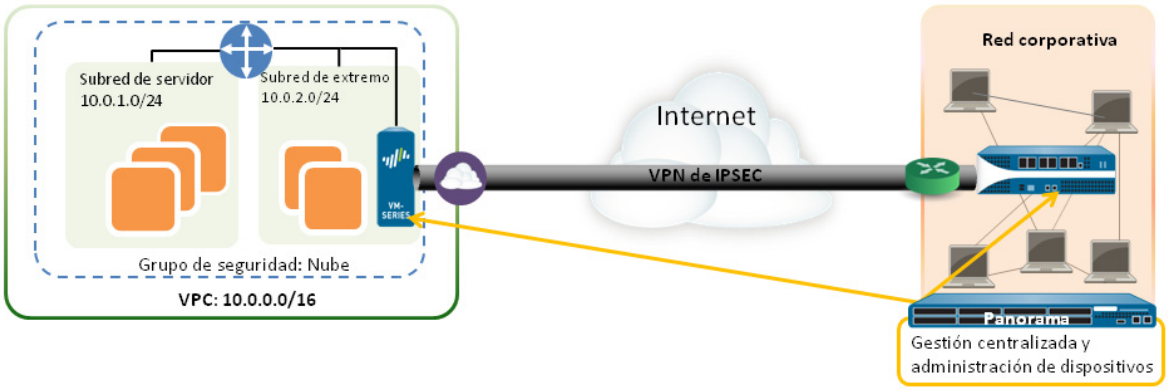
  Cuando los usuarios necesitan acceder a las aplicaciones en la subred privada, el cortafuegos recibe la solicitud y la dirige a la aplicación apropiada, tras verificar la política de seguridad y realizar la NAT de destino. En la ruta de retorno, el cortafuegos recibe el tráfico, aplica la política de seguridad y usa la NAT de origen para entregar el contenido al usuario. Consulte Caso de uso: Protección de las instancias de EC2 en AWS Cloud.



- Implemente el cortafuegos VM-Series para obtener acceso VPN entre la red corporativa y las instancias de EC2 dentro de la AWS Virtual Private Cloud.

  Para conectar su red corporativa con las aplicaciones implementadas en la AWS Cloud, puede configurar el cortafuegos como un punto de terminación para un túnel VPN de IPSec. Este túnel VPN permite a los usuarios en su red para acceder de forma segura a las aplicaciones en la nube.

  Para la gestión centralizada, el forzaje consistente de políticas en toda su red y la creación centralizada de logs e informes, también puede implementar Panorama en su red corporativa. Si necesita configurar el acceso VPN a VPC múltiples, el uso de Panorama le permite agrupar los cortafuegos por regiones y administrarlos de forma sencilla.



- Implemente el cortafuegos VM-Series como una puerta de enlace de GlobalProtect para permitir el acceso a usuarios remotos de forma segura desde ordenadores portátiles. El agente de GlobalProtect en el portátil conecta con la puerta de enlace, y basándose en la solicitud, la puerta de enlace configura una conexión de VPN a la red corporativa o enruta la solicitud a Internet. Para aplicar el cumplimiento con la seguridad para usuarios de dispositivos móviles (mediante el uso de la aplicación GlobalProtect), la puerta de enlace de GlobalProtect se usa junto con el gestor de seguridad móvil de GlobalProtect. El gestor de seguridad móvil de GlobalProtect garantiza que los dispositivos se gestionen y configuren con la configuración del dispositivo y la información de cuentas para su uso con aplicaciones y redes corporativas.

Implementación del cortafuegos VM-Series en AWS

- Obtención de la AMI
- Consulte los requisitos y limitaciones del sistema para VM-Series en AWS
- Hoja de trabajo para la planificación de VM-Series en la VPC de AWS
- Inicio del cortafuegos VM-Series en AWS

Obtención de la AMI

La AMI para el cortafuegos VM-Series está disponible en el AWS Marketplace con la tarifa para licencias existentes (Bring Your Own License, BYOL). Para adquirir licencias, póngase en contacto con su ingeniero de sistemas de Palo Alto Networks o distribuidor.

Consulte los requisitos y limitaciones del sistema para VM-Series en AWS

Requisito	Detalles
Tipos de instancia de EC2	Implemente el cortafuegos VM-Series en una de las siguientes instancias de EC2: • m3.xlarge • m3.2xlarge • c3.xlarge • c3.2xlarge • c3.4xlarge • c3.8xlarge Los requisitos mínimos de los recursos para el cortafuegos VM-Series son: vCPU: 2; Memoria: 4 GB; 5 GB para el VM-1000-HV; Disco: 40 GB. Si implementa el cortafuegos VM-Series en un tipo de instancia de EC2 que no cumple estos requisitos, el cortafuegos se reiniciará en el modo de mantenimiento.
Amazon Elastic Block Storage (EBS)	El cortafuegos VM-Series debe usar el volumen de almacenamiento Amazon Elastic Block Storage (EBS). La optimización de EBS ofrece una pila de configuración optimizada y capacidad dedicada y adicional para la E/S de Amazon EBS.
Redes	Dado que AWS sólo admite funciones de red de capa 3, el cortafuegos VM-Series sólo se puede implementar con interfaces de capa 3. Las interfaces de capa 2, Virtual Wire, VLAN y las subinterfaces no son compatibles con los cortafuegos VM-Series implementados en la VPC de AWS.

Requisito	Detalles
Interfaces	Compatibilidad para un total de ocho interfaces: una interfaz de gestión y un máximo de siete interfaces de red elástica (ENI) para tráfico de datos. El cortafuegos VM-Series no es compatible con la adición en caliente de ENI; para detectar la adición o eliminación de una ENI, debe reiniciar el cortafuegos. La instancia de EC2 que elija determinará el número total de ENI que puede habilitar. Por ejemplo, c3.8xlarge admite ocho (8) ENI.
Derechos de asistencia y licencias	Se necesita una cuenta de asistencia y una licencia VM-Series válida para obtener el archivo Amazon Machine Image (AMI), necesario para instalar el cortafuegos VM-Series en la VPC de AWS. Las licencias necesarias para el cortafuegos VM-Series (licencia de capacidad, licencia de asistencia y suscripciones para la prevención de amenazas, filtrado de URL, WildFire, etc.) deben adquirirse en Palo Alto Networks. Para adquirir las licencias para su implementación, póngase en contacto con su representante de ventas.

Hoja de trabajo para la planificación de VM-Series en la VPC de AWS

Para facilitar la implementación, planifique las subredes de la VPC y las instancias de EC2 que quiere implementar en cada subred. Antes de empezar, use la siguiente tabla para cotejar la información de red necesaria para implementar e insertar los cortafuegos VM-Series en el flujo de tráfico de VPC:

Elemento de configuración	Valor
CIDR de VPC	
Grupos de seguridad	
CIDR de subred (pública)	
CIDR de subred (privada)	
Tabla de enrutamiento de subred (pública)	
Tabla de enrutamiento de subred (privada)	
Grupos de seguridad • Reglas de configuración del acceso a la gestión del cortafuegos (eth0/0) • Reglas de acceso a las interfaces del plano de datos del cortafuegos • Reglas para el acceso a las interfaces asignadas a los servidores de aplicaciones.	

Elemento de configuración	Valor
Instancia 1 de EC2 (cortafuegos VM-Series) Sólo se requiere una EIP para la interfaz de plano de datos adjuntada a la subred pública.	Subred: Tipo de instancia: IP de interfaz de gestión: EIP de interfaz de gestión: Interfaz de plano de datos eth1/1 • IP privada: • EIP (en caso necesario): • Grupo de seguridad: Interfaz de plano de datos eth1/2 • IP privada: • EIP (en caso necesario): • Grupo de seguridad:
Instancia 2 de EC2 (aplicación que se va a proteger) Repita este conjunto de valores para las aplicaciones adicionales que se implementen.	Subred: Tipo de instancia: IP de interfaz de gestión: Puerta de enlace predeterminada: Interfaz de plano de datos 1 • IP privada

Inicio del cortafuegos VM-Series en AWS

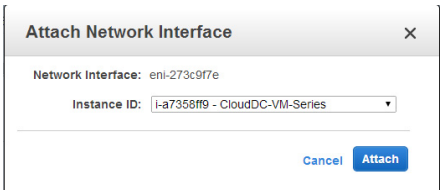
Si no ha registrado todavía el código de autenticación de capacidad que ha recibido con el correo electrónico de cumplimiento del pedido, con su cuenta de asistencia, consulte Registro del cortafuegos VM-Series. Una vez registrado, implemente el cortafuegos VM-Series iniciándolo en la VPC de AWS del siguiente modo:

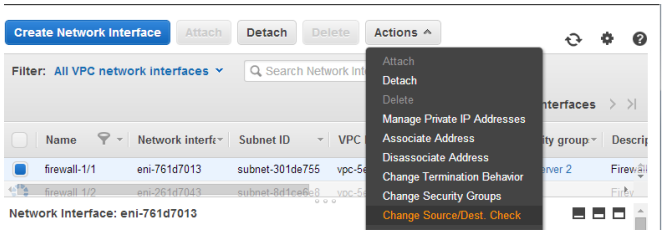
Inicio del cortafuegos VM-Series en la VPC de AWS	
Paso 1 Acceda a la consola de AWS.	Inicie sesión en la consola de AWS y seleccione el panel EC2.

Inicio del cortafuegos VM-Series en la VPC de AWS (Continuación)		
Paso 2	Configure la VPC según sus necesidades de red. Tanto si inicia el cortafuegos VM-Series en una VPC existente o crea una nueva VPC, el cortafuegos VM-Series debe poder recibir tráfico desde las instancias de EC2 y realizar comunicaciones de entrada y salida entre la VPC e Internet. Consulte las instrucciones para crear una VPC y configurar el acceso a la misma en la documentación de la VPC de AWS. En Caso de uso: Protección de las instancias de EC2 en AWS Cloud puede consultar un ejemplo con un flujo de trabajo completo.	1. Cree una nueva VPC o use una existente. 2. Compruebe que los componentes de red y seguridad están definidos adecuadamente. • Habilite la comunicación con Internet. La VPC predeterminada incluye una puerta de enlace de Internet, y si instala el cortafuegos VM-Series en la subred predeterminada, tendrá acceso a Internet. • Cree subredes. Las subredes son segmentos de intervalos de direcciones IP asignados a la VPC en las que puede iniciar las instancias de EC2. El cortafuegos VM-Series debe pertenecer a la subred pública para que se pueda configurar su acceso a Internet. • Cree grupos de seguridad según sea necesario para gestionar el tráfico entrante y saliente desde las instancias o subredes de EC2. • Añada rutas a la tabla de enrutamiento para una subred privada para garantizar que el tráfico se puede enrutar a través de subredes y grupos de seguridad en la VPC, según corresponda.

Inicio del cortafuegos VM-Series en la VPC de AWS (Continuación)	
Paso 3 Inicie el cortafuegos VM-Series.	1. En el panel EC2, haga clic en **Iniciar instancia**. 2. Seleccione la AMI de VM-Series. Para obtener la AMI, consulte Obtención de la AMI. 3. Inicie el cortafuegos VM-Series en la instancia de EC2. a. Elija el **tipo de instancia de EC2** (m3.xlarge, c3.xlarge o c3.8xlarge) para asignar los recursos requeridos para el cortafuegos y haga clic en **Siguiente**. b. Seleccione la VPC. c. Seleccione la subred pública a la que se adjuntará la interfaz de gestión de VM-Series. d. Seleccione **Asignar automáticamente una dirección IP pública**. Esto le permite obtener una dirección IP de acceso público para la interfaz de gestión del cortafuegos VM-Series. Posteriormente, puede adjuntar una dirección IP elástica a la interfaz de gestión; a diferencia de la dirección IP pública, que deshace la asociación con el cortafuegos cuando se finaliza la instancia, la dirección IP elástica ofrece continuidad y se puede volver a adjuntar a una nueva instancia (o una de sustitución) del cortafuegos VM-Series sin necesidad de volver a configurar la dirección IP, independientemente de la ubicación de referencia que tenga. e. Seleccione **Iniciar como instancia optimizada para EBS**. f. Acepte la configuración de **almacenamiento** predeterminada. g. Omita el etiquetado. Podrá añadir etiquetas en otro momento. h. Seleccione un **Grupo de seguridad** existente o cree uno nuevo. Este grupo de seguridad sirve para restringir el acceso a la interfaz de gestión del cortafuegos. i. Si se le solicita, seleccione una opción de **SSD** adecuada para su configuración. j. Seleccione **Revisar e iniciar**. Revise que sus selecciones son precisas y haga clic en **Iniciar** k. Seleccione un par de claves existente o cree uno nuevo y acepte el descargo de responsabilidad de claves. l. Descargue y guarde la clave privada en un lugar seguro; la extensión del archivo es `.pem`. Si pierde la clave, no se puede volver a regenerar. Lleva entre 5 y 7 minutos iniciar el cortafuegos VM-Series. Puede consultar el progreso en el panel EC2. Al completar el proceso, el cortafuegos VM-Series se muestra en la página **Instancias** del panel EC2.
Aunque puede añadir interfaces de red adicionales al cortafuegos VM-Series al iniciarlo, para reducir al mínimo los problemas de implementación de la instancia, adjunte interfaces de red adicionales después de iniciar el cortafuegos.	
La primera vez que se accede al cortafuegos se solicita este par de claves. También es necesario acceder al cortafuegos en el modo de mantenimiento.	

Inicio del cortafuegos VM-Series en la VPC de AWS (Continuación)

Paso 4 Configure una nueva contraseña de administración para el cortafuegos. La contraseña predeterminada es admin. Mediante la CLI, debe configurar una contraseña única para el cortafuegos antes de poder acceder a la interfaz web del mismo.	1. Use una dirección IP pública para hacer SSH en la interfaz de línea de comando (CLI) del cortafuegos VM-Series. Necesitará la clave privada que usó o creó en el Paso 3-k para acceder a la CLI. 2. Introduzca el siguiente comando para iniciar sesión en el cortafuegos: **ssh -i** <*clave_privada.pem*> **admin@**<*dirección_ip-pública*> 3. Configure una nueva contraseña usando el siguiente comando y siga las indicaciones en pantalla: **configure** **set mgt-config users admin password** **commit** 4. Finalice la sesión SSH.
Paso 5 Apague el cortafuegos VM-Series.	1. En el panel EC2, seleccione **Instancias**. 2. En la lista, seleccione el cortafuegos VM-Series y haga clic en **Acciones > Detener**.
Paso 6 Cree interfaces de red virtuales y adjúntelas al cortafuegos VM-Series Las interfaces de red virtuales se llaman Interfaces de red elásticas (ENI) en AWS, y actúan como interfaces de red de plano de datos en el cortafuegos. Estas interfaces se usan para la gestión del tráfico de datos desde o hacia el cortafuegos. Necesitará al menos dos ENI. Puede añadir hasta siete ENI para gestionar el tráfico de datos en el cortafuegos VM-Series; compruebe su tipo de instancia de EC2 para comprobar el número máximo que admite. Para detectar las ENI adjuntadas recientemente, se necesita reiniciar el cortafuegos VM-Series. Si aún no ha apagado el cortafuegos, continúe con el proceso de activación de licencia, que ordena un reinicio del cortafuegos. Durante el reinicio del cortafuegos se detectan las ENI.	1. En el panel EC2, seleccione **Interfaces de red** y haga clic en **Crear interfaces de red**. 2. Introduzca un nombre descriptivo para la interfaz. 3. Seleccione la subred. Use el ID de subred para asegurarse de que ha seleccionado la subred correcta. Sólo puede adjuntar una ENI a una instancia en la misma subred. 4. Introduzca la dirección de **IP privada** para asignarla a la interfaz y seleccione **Asignar automáticamente** para asignar automáticamente una dirección IP dentro de las direcciones IP disponibles en la subred seleccionada. 5. Seleccione el **grupo de seguridad** para controlar el acceso a la interfaz de red del plano de datos. 6. Haga clic en **Sí, crear**. 7. Para adjuntar la ENI al cortafuegos VM-Series, seleccione la interfaz que acaba de crear y haga clic en **Adjuntar**.  8. Seleccione el **ID de instancia** del cortafuegos VM-Series y haga clic en **Adjuntar**. 9. Repita los pasos anteriores para crear y adjuntar al menos una ENI más al cortafuegos.

Inicio del cortafuegos VM-Series en la VPC de AWS (Continuación)		
Paso 7	Active las licencias del cortafuegos VM-Series. Esta tarea no se realiza en la consola de gestión de AWS. Necesita acceder al portal de asistencia de Palo Alto Networks y a la interfaz web del cortafuegos VM-Series para activar la licencia.	Consulte Activación de la licencia.
Paso 8	Deshabilite la comprobación de origen/destino en todas las interfaces de red de planos de datos del cortafuegos. Si deshabilita esta opción, permite a la interfaz gestionar el tráfico de red no destinado a la dirección IP asignada a la interfaz de red.	1. En el panel EC2, seleccione la interfaz de red, por ejemplo, eth1/1, en la pestaña **Interfaces de red**. 2. En el menú desplegable **Acción**, seleccione **Cambiar comprobación de origen/dest.**  3. Haga clic en **Deshabilitado** y **guarde** los cambios. 4. Repita los pasos 1-3 con cada interfaz de plano de datos del cortafuegos.

Inicio del cortafuegos VM-Series en la VPC de AWS (Continuación)

Paso 9 Configure las interfaces de red del plano de datos como interfaces de capa 3 en el cortafuegos.

Para ver una configuración de ejemplo, consulte desde el paso Paso 14 hasta el Paso 17 de Caso de uso: Protección de las instancias de EC2 en AWS Cloud.

En los servidores de aplicaciones dentro de la VPC, defina la interfaz de red de plano de datos del cortafuegos como la puerta de enlace predeterminada.

1. Inicie un navegador web e introduzca la dirección IP pública o la EIP asignada a la interfaz de gestión del cortafuegos VM-Series.
2. Seleccione **Red > Interfaces > Ethernet**.

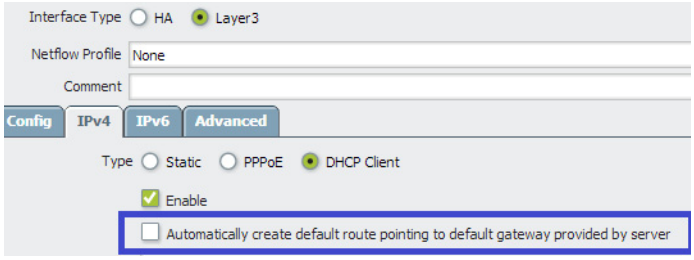
   Antes de iniciar la configuración de las interfaces de red, compruebe que el estado de enlace de la interfaz está activo.

. Si el estado de enlace no está activo, reinicie el cortafuegos.
3. Haga clic en el enlace de **ethernet 1/1** y configúrelo del siguiente modo:
   - **Tipo de interfaz**: **Capa3**
   - En la pestaña **Configurar**, asigne la interfaz el router predeterminado.
   - En la pestaña **Configurar**, amplíe el menú desplegable **Zona de seguridad** y seleccione **Nueva zona**. Defina una nueva zona, por ejemplo, VM_Series_untrust, y a continuación haga clic en **ACEPTAR**.
   - En la pestaña **IPv4**, seleccione **Estático** o **Cliente DHCP**.

     Si usa la opción **Estático**, haga clic en **Añadir** en la sección IP e introduzca la dirección IP y la máscara de red para la interfaz; por ejemplo, 10.0.0.10/24.
     Asegúrese de que la dirección IP coincide con la dirección IP de la ENI que ha asignado anteriormente.

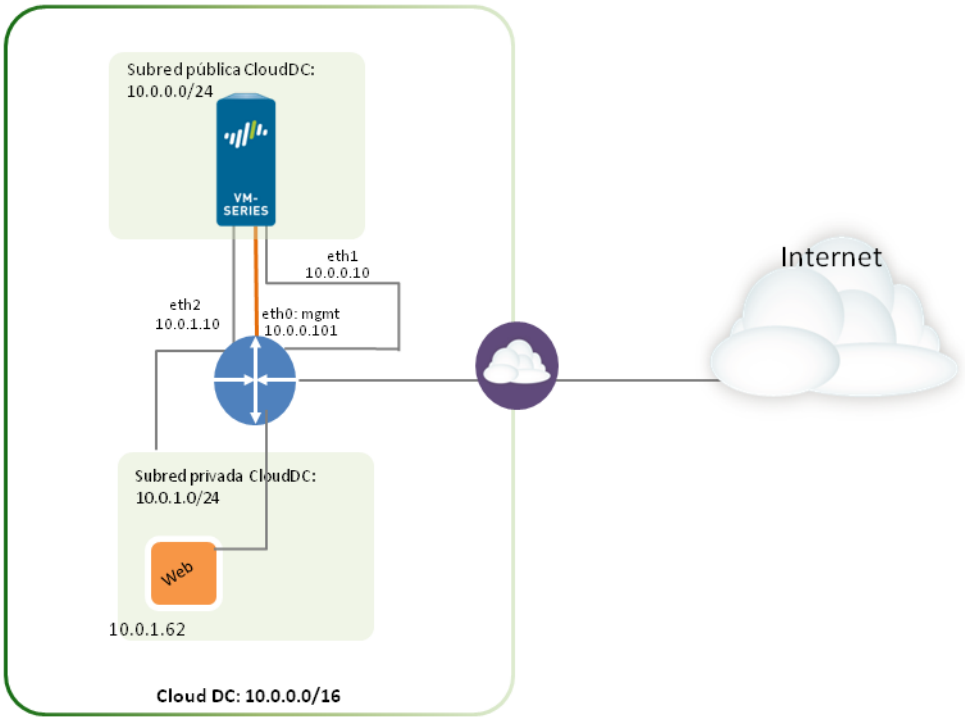
     Si usa DHCP, seleccione **Cliente DHCP**; la dirección IP privada que ha asignado a la ENI en la consola de gestión de AWS se adquirirá de manera automática.
4. Haga clic en el enlace de **ethernet 1/2** y configúrelo del siguiente modo:
   - **Tipo de interfaz**: **Capa3**
   - **Zona de seguridad: VM_Series_trust**
   - **Dirección IP**: Seleccione el botón de opción **Estático** o **Cliente DHCP**.

     Para Estático, haga clic en **Añadir** en la sección IP e introduzca la dirección IP y la máscara de red para la interfaz. Asegúrese de que la dirección IP coincide con la dirección IP de la ENI adjuntada que ha asignado anteriormente.

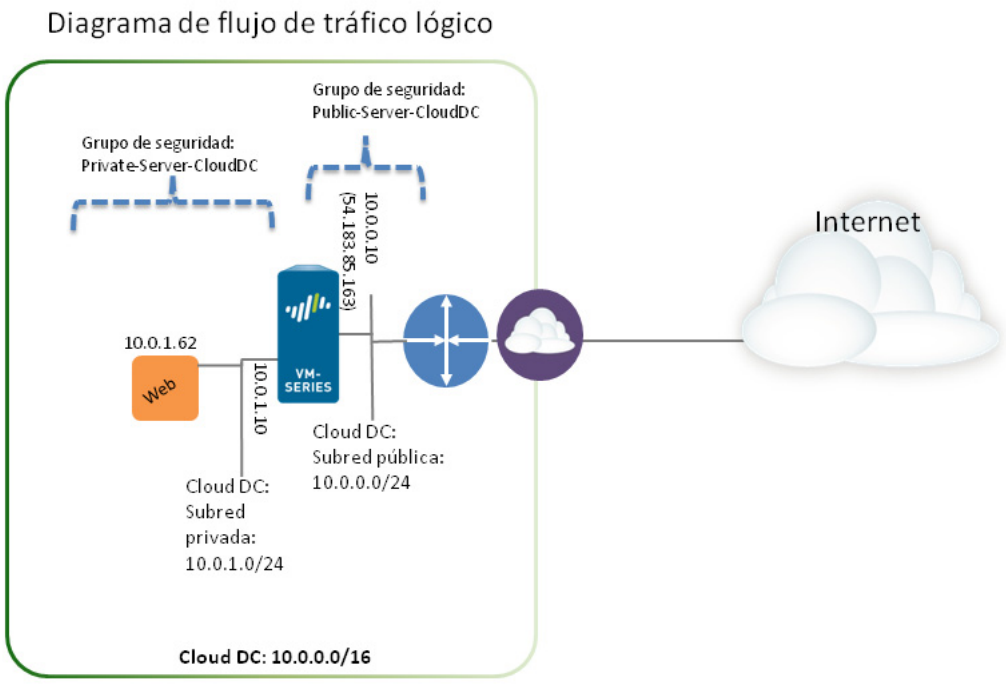
Inicio del cortafuegos VM-Series en la VPC de AWS (Continuación)	
	Para DHCP, anule la selección de la casilla de verificación **Crear automáticamente ruta predeterminada a la puerta de enlace predeterminada proporcionada por el servidor**. Para una interfaz adjuntada a la subred privada en la VPC, deshabilitar esta opción garantiza que el tráfico gestionado por esta interfaz no fluya directamente a la puerta de enlace de Internet en la VPC. 
Paso 10 Cree reglas NAT para permitir el tráfico entrante y saliente desde servidores implementados dentro de la VPC.	1. Seleccione **Políticas > NAT** en la interfaz web del cortafuegos. 2. Cree una regla NAT para permitir el tráfico desde la interfaz de red del plano de datos en el cortafuegos a la interfaz del servidor web en la VPC. 3. Cree una regla NAT para permitir el acceso saliente para el tráfico desde el servidor web a Internet.
Paso 11 Cree políticas de seguridad para permitir/denegar el tráfico entrante y saliente desde servidores implementados dentro de la VPC.	1. Seleccione **Políticas > Seguridad** en la interfaz web del cortafuegos. 2. Haga clic en **Añadir**, y especifique las zonas, aplicaciones y opciones de inicio de sesión que le gustaría ejecutar para restringir el tráfico de auditoría que atraviesa la red.
Paso 12 Compile los cambios en el cortafuegos.	1. Haga clic en **Compilar**.
Paso 13 Compruebe que el cortafuegos VM-Series protege el tráfico y que las reglas NAT están en vigor.	1. Seleccione **Supervisar > Logs > Tráfico** en la interfaz web del cortafuegos. 2. Consulte los logs para asegurarse de que las aplicaciones que atraviesan la red cumplen las políticas de seguridad que ha implementado.

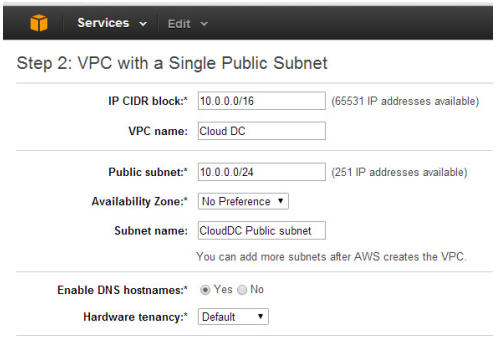
Caso de uso: Protección de las instancias de EC2 en AWS Cloud

En este ejemplo, la VPC se implementa en la red 10.0.0.0/16 con dos subredes /24: 10.0.0.0/24 y 10.0.1.0/24. El cortafuegos VM-Series se iniciará en la subred 10.0.0.0/24 a la que se ha adjuntado la puerta de enlace de Internet. La subred 10.0.1.0/24 es una subred privada que alojará las instancias de EC2 que necesitan la protección del cortafuegos VM-Series; cualquier servidor en esta subred privada usa NAT para una dirección IP enrutable (que es una dirección IP elástica) para acceder a Internet. Use la Hoja de trabajo para la planificación de VM-Series en la VPC de AWS para planificar el diseño de la VPC; la grabación de los intervalos de subred, las interfaces de red y las direcciones IP asociadas para las instancias de EC2 y los grupos de seguridad facilitará y optimizará el proceso de configuración.

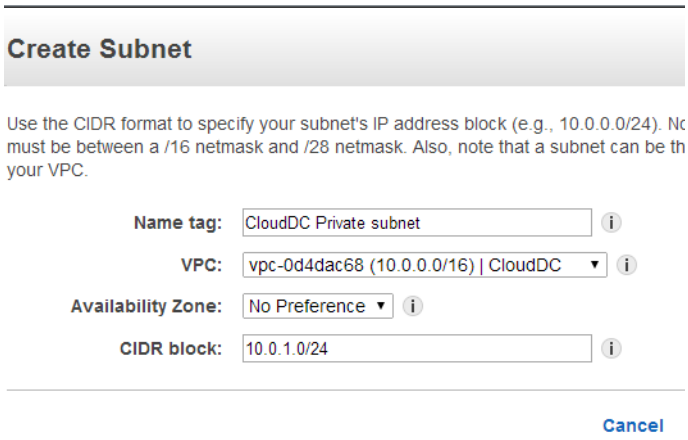
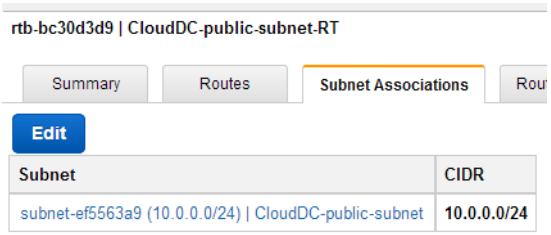


La siguiente imagen ilustra el flujo lógico de tráfico hacia y desde el servidor web a Internet. El tráfico hacia y desde el servidor web se envía a la interfaz de datos del cortafuegos VM-Series adjunto a la subred privada. El cortafuegos aplica políticas y procesos de tráfico entrante y saliente hacia y desde la puerta de enlace de Internet del VPC. La imagen muestra también los grupos de seguridad adjuntos a las interfaces de datos.



Implementación del cortafuegos VM-Series como una puerta de enlace de la nube	
Paso 1 Cree una nueva VPC con una subred pública (o seleccione una VPC existente).	1. Inicie sesión en la consola de AWS y seleccione el panel **VPC**. 2. Compruebe que ha seleccionado el área geográfica correcta (región de AWS). La VPC se implementará en la región seleccionada actualmente. 3. Seleccione **Iniciar asistente de VPC** y seleccione **VPC con una subred pública sencilla**. En este ejemplo, el bloque CIDR de IP para la VPC es 10.0.0.0/16, el nombre de la VPC es Cloud DC, la subred pública es 10.0.0.0/24 y el nombre de la subred es Cloud DC Public subnet. Creará una subred privada después de crear la VPC.  4. Haga clic en **Crear VPC**.

Implementación del cortafuegos VM-Series como una puerta de enlace de la nube (Continuación)

Paso 2 Cree una subred privada.	Seleccione **Subredes** y haga clic en **Crear una subred**. Introduzca la información. En este ejemplo, la **etiqueta de nombre** para la subred es Web/DB Server Subnet, se crea en la VPC del Cloud Datacenter y se asigna un bloque CIDR de 10.0.1.0/24. 
Paso 3 Cree una nueva tabla de enrutamiento para cada subred. Aunque se crea automáticamente una tabla de enrutamiento en la VPC, recomendamos crear nuevas tablas de enrutamiento en lugar de modificar la tabla de enrutamiento predeterminada. Para dirigir el tráfico saliente desde cada subred, en un punto posterior de este flujo de trabajo añadirá las rutas a la tabla de enrutamiento asociada a cada subred.	1. Seleccione **Tablas de enrutamiento** > **Crear tabla de enrutamiento**. 2. Añada un **nombre**; por ejemplo, CloudDC-public-subnet-RT, seleccione la **VPC** que creó en el Paso 1 y haga clic en **Sí, crear**. 3. Seleccione la tabla de enrutamiento, haga clic en **Asociaciones de subred** y seleccione la subred pública.  4. Seleccione **Crear tabla de enrutamiento**. 5. Añada un **nombre**; por ejemplo, CloudDC-private-subnet-RT, seleccione la **VPC** que creó en el Paso 1 y haga clic en **Sí, crear**. 6. Seleccione la tabla de enrutamiento, haga clic en **Asociaciones de subred** y seleccione la subred privada.

Implementación del cortafuegos VM-Series como una puerta de enlace de la nube (Continuación)

Paso 4 Cree grupos de seguridad para restringir el acceso a Internet entrante/saliente a las instancias de EC2 en la VPC. De manera predeterminada, AWS no permite la comunicación entre interfaces que no pertenezcan al mismo grupo de seguridad.	Seleccione **Grupos de seguridad** y haga clic en el botón **Crear grupo de seguridad**. En este ejemplo, hemos creado tres grupos de seguridad con las siguientes reglas para acceso entrante: • CloudDC-Management, que especifica los protocolos y las direcciones IP de origen que pueden conectarse a la interfaz de gestión en el cortafuegos VM-Series. Necesita SSH y HTTPS como mínimo. En este ejemplo, se habilitan SSH, ICMP, HTTP y HTTPS en las interfaces de red adjuntas a este grupo de seguridad. La interfaz de gestión (eth 0/0) del cortafuegos VM-Series se asignará a CloudDC-management-sg. • Public-Server-CloudDC, que especifica las direcciones IP que se pueden conectar a través de HTTP, FTP y SSH en la VPC. Este grupo permite el tráfico desde la red externa al cortafuegos. La interfaz del plano de datos eth 1/1 del cortafuegos VM-Series se asignará a Public-Server-CloudDC. • Private-Server-CloudDC, con acceso muy limitado. Sólo permite que las instancias de EC2 en la misma subred se comuniquen entre sí y con el cortafuegos VM-Series. La interfaz del plano de datos eth1/2 del cortafuegos VM-Series y la aplicación en la subred privada se adjuntarán a este grupo de seguridad.

Name tag	Group ID	Group Name	VPC	Description
CloudDC-private-subnet-sg	sg-6c32c409	Private-Server-CloudDC	vpc-0d4dac68 (10.0.0.0/16) |...	For Private Servers to comm...
CloudDC-public-subnet-sg	sg-6832c40d	Public-Server-CloudDC	vpc-0d4dac68 (10.0.0.0/16) |...	External Traffic to VM-Series
CloudDC-management-sg	sg-9735c3f2	CloudDC-Managment	vpc-0d4dac68 (10.0.0.0/16) |...	CloudDC-Management
	sg-1035c375	default	vpc-0d4dac68 (10.0.0.0/16) |...	default VPC security group

Paso 5 Implemente el cortafuegos VM-Series. Sólo la interfaz de red principal que actuará como la interfaz de gestión se adjuntará y configurará para el cortafuegos durante el primer inicio. Las interfaces de red necesarias para la gestión del tráfico de datos se añadirá en el Paso 6.	Consulte el Paso 3 en Inicio del cortafuegos VM-Series en AWS.

Implementación del cortafuegos VM-Series como una puerta de enlace de la nube (Continuación)

Paso 6 Cree y adjunte las interfaces de red virtual, denominadas interfaces de red elásticas (ENI), al cortafuegos VM-Series. Estas ENI se usan para la gestión del tráfico de datos desde o hacia el cortafuegos.

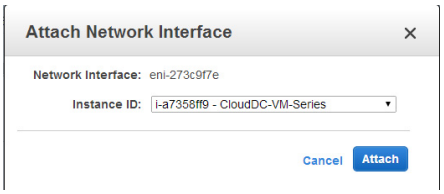
1. En el panel EC2, seleccione **Interfaces de red** y haga clic en **Crear interfaces de red**.
2. Introduzca un nombre descriptivo para la interfaz.
3. Seleccione la subred. Use el ID de subred para asegurarse de que ha seleccionado la subred correcta. Sólo puede adjuntar una ENI a una instancia en la misma subred.
4. Introduzca la dirección de **IP privada** que quiere asignar a la interfaz o seleccione **Asignar automáticamente** para asignar automáticamente una dirección IP dentro de las direcciones IP disponibles en la subred seleccionada.
5. Seleccione el **grupo de seguridad** para controlar el acceso a la interfaz de red.
6. Haga clic en **Sí, crear**.

   En este ejemplo, se crean dos interfaces con la siguiente configuración:

Name	Network interfa	Subnet ID	VPC ID	Zone	Security group	Description	Instance ID
CloudDC-VM-Series-Untrust	eni-bcf355e5	subnet-ef5563a9	vpc-0d4dac68	us-west-1a	Public-Server-...	CloudDC-VM-Series-untrust	i-a7358ff9
CloudDC-VM-Series-Trust	eni-abf355f2	subnet-f75563b1	vpc-0d4dac68	us-west-1a	Private-Server-...	CloudDC-VM-Series-Trust	i-a7358ff9

   - Para Eth1/1 (VM-Series-Untrust)
     - Subred: 10.0.0.0/24
     - IP privada:10.0.0.10
     - Grupo de seguridad: Public-Server-CloudDC
   - Para Eth1/2 (VM-Series-Trust)
     - Subred: 10.0.1.0/24
     - IP privada:10.0.1.10
     - Grupo de seguridad: Private-Server-CloudDC

7. Para adjuntar la ENI al cortafuegos VM-Series, seleccione la interfaz que acaba de crear y haga clic en **Adjuntar**.



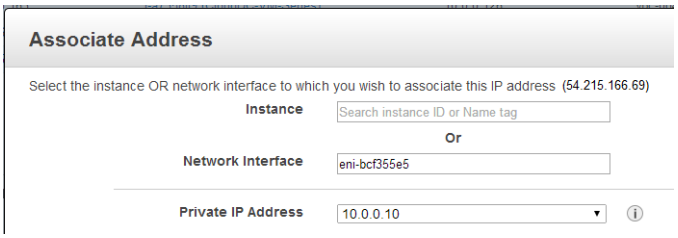
8. Seleccione el **ID de instancia** del cortafuegos VM-Series y haga clic en **Adjuntar**.
9. Repita los pasos 7 y 8 para adjuntar la otra interfaz de red.

Implementación del cortafuegos VM-Series como una puerta de enlace de la nube (Continuación)

Paso 7 Cree una dirección IP elástica y adjúntela a la interfaz de red de plano de datos del cortafuegos que requiere acceso directo a Internet.

En este ejemplo, VM-Series_Untrust se asigna a una EIP. La EIP asociada a la interfaz es la dirección IP de acceso público para el servidor web en la subred privada.

1. Seleccione **IP elásticas** y haga clic en **Asignar nueva dirección**.
2. Seleccione **EC2-VPC** y haga clic en **Sí, asignar**.
3. Seleccione la EIP recién asignada y haga clic en **Asociar dirección**.
4. Seleccione la **interfaz de red** y la **dirección IP privada** asociada con la interfaz y haga clic en **Sí, asociar**.



En este ejemplo, la configuración es:

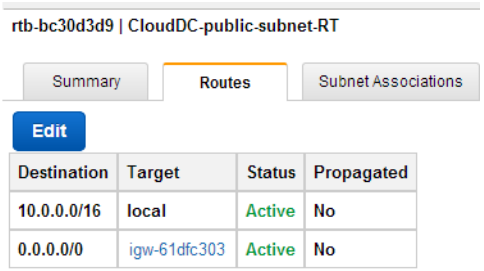
Address	Instance	Private IP Address	Scope	Public DNS
54.183.85.163	i-a7358ff9 (CloudDC-VM-Series)	10.0.0.126	vpc-0d4dac68	ec2-54-183-85-163.us-west-...
54.215.166.69	i-a7358ff9 (CloudDC-VM-Series)	10.0.0.10	vpc-0d4dac68	ec2-54-215-166-69.us-west-...

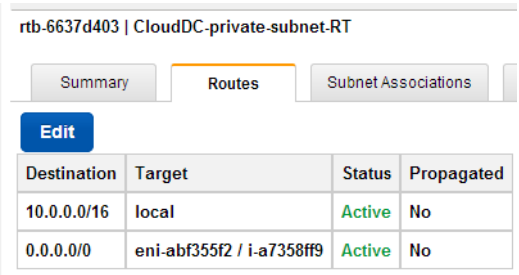
Paso 8 Deshabilite la comprobación de Origen/Destino en cada interfaz de red adjuntada al cortafuegos VM-Series. Deshabilitar este atributo permite a la interfaz gestionar el tráfico de red no destinado a su dirección IP.

1. Seleccione la interfaz de red en la pestaña **Interfaces de red**.
2. En el menú desplegable **Acción**, seleccione **Cambiar comprobación de origen/dest.**
3. Haga clic en **Deshabilitado** y **guarde** los cambios.
4. Repita los pasos 1-3 para interfaces de red adicionales, firewall-1/2 en este ejemplo.

Paso 9 En la tabla de enrutamiento asociada a la subred pública (desde el Paso 3), añada una ruta predeterminada a la puerta de enlace de Internet para la VPC.

1. Desde el panel VPC, seleccione **Tablas de enrutamiento** y busque la tabla de enrutamiento asociada a la subred pública.
2. Seleccione la tabla de enrutamiento, seleccione **Rutas** y haga clic en **Editar**.
3. Añada una ruta para reenviar paquetes desde esta subred a la puerta de enlace de Internet. En este ejemplo, 0.0.0.0/0 indica que todo el tráfico desde o hacia esta subred usará la puerta de enlace de Internet adjuntada a la VPC.



Implementación del cortafuegos VM-Series como una puerta de enlace de la nube (Continuación)	
Paso 10 En la tabla de enrutamiento asociada a la subred pública, añada una ruta predeterminada para enviar tráfico al cortafuegos VM-Series. Añadir esta ruta permite el reenvío de tráfico desde instancias de EC2 en esta subred privada al cortafuegos VM-Series.	1. Desde el panel VPC, seleccione **Tablas de enrutamiento** y busque la tabla de enrutamiento asociada a la subred privada. 2. Seleccione la tabla de enrutamiento, seleccione **Rutas** y haga clic en **Editar**. 3. Añada una ruta para reenviar paquetes desde esta subred a la interfaz de red del cortafuegos VM-Series que reside en la misma subred. En este ejemplo, 0.0.0.0/0 indica que todo el tráfico desde y hacia esta subred usará eni-abf355f2 (ethernet 1/2, que es CloudDC-VM-Series-Trust) en el cortafuegos VM-Series.  Por cada servidor web o de base de datos implementado en una instancia de EC2 en la subred privada, debe añadir también la dirección IP del cortafuegos VM-Series como la puerta de enlace predeterminada.
Realice del Paso 11 al Paso 16 en el cortafuegos VM-Series	
Paso 11 Configure una nueva contraseña de administración para el cortafuegos. Se necesita una herramienta SSH como PuTTY para acceder a la CLI en el cortafuegos y cambiar la contraseña administrativa predeterminada. No puede acceder a la interfaz web hasta que haga SSH y cambie la contraseña predeterminada.	1. Use la dirección IP pública que ha configurado en el cortafuegos para hacer SSH en la interfaz de línea de comando (CLI) del cortafuegos VM-Series. Necesitará la clave privada que usó o creó en Inicie el cortafuegos VM-Series., Paso 3-k para acceder a la CLI. 2. Introduzca el siguiente comando para iniciar sesión en el cortafuegos: **`ssh-i`** *<nombre_clave_privada>* **`admin@`***<dirección_ip-pública>* 3. Configure una nueva contraseña usando el siguiente comando y siga las indicaciones en pantalla: **`set password`** **`configure`** **`commit`** 4. Finalice la sesión SSH.
Paso 12 Acceda a la interfaz web del cortafuegos VM-Series.	Abra un navegador web e introduzca la dirección IP pública o la EIP de la interfaz de gestión. Por ejemplo: https://54.183.85.163
Paso 13 Active las licencias del cortafuegos VM-Series.	Consulte Activación de la licencia.

Implementación del cortafuegos VM-Series como una puerta de enlace de la nube (Continuación)

Paso 14 En el cortafuegos VM-Series, configure las interfaces de red del plano de datos en el cortafuegos como interfaces de capa 3.

1. Seleccione **Red > Interfaces > Ethernet**.

Antes de iniciar la configuración de las interfaces de red, compruebe que el estado de enlace de la interfaz está activo.

. Si el estado de enlace no está activo, reinicie el cortafuegos.

2. Haga clic en el enlace de **ethernet 1/1** y configúrelo del siguiente modo:
   - **Tipo de interfaz**: **Capa3**
   - Seleccione la pestaña **Configurar** y asigne la interfaz el router predeterminado.
   - En la pestaña **Configurar**, amplíe el menú desplegable **Zona de seguridad** y seleccione **Nueva zona**. Defina una zona nueva (p. ej., untrust) y, a continuación, haga clic en **ACEPTAR**.
   - Seleccione **IPv4**, seleccione **Cliente DHCP**; la adquisición de la dirección IP privada que asignó a la interfaz de red en la consola de gestión de AWS se realizará automáticamente.
   - En la pestaña **Avanzada > Otra información**, amplíe el menú desplegable Perfil de gestión y seleccione **Nuevo perfil de gestión**.
   - Introduzca un **nombre** para el perfil, como allow_ping, y seleccione **Ping** en la lista de servicios permitidos; a continuación, haga clic en **ACEPTAR**.
   - Para guardar la configuración de la interfaz, haga clic en **Aceptar**.
3. Haga clic en el enlace de **ethernet 1/2** y configúrelo del siguiente modo:
   - **Tipo de interfaz**: **Capa3**
   - Seleccione la pestaña **Configurar** y asigne la interfaz el router predeterminado.
   - En la pestaña **Configurar**, amplíe el menú desplegable **Zona de seguridad** y seleccione **Nueva zona**. Defina una zona nueva (p. ej., trust) y, a continuación, haga clic en **ACEPTAR**.
   - Seleccione **IPv4**, seleccione **Cliente DHCP**.
   - En la pestaña **IPv4**, anule la selección de la casilla de verificación **Crear automáticamente ruta predeterminada a la puerta de enlace predeterminada proporcionada por el servidor**. Para una interfaz adjuntada a la subred privada en la VPC, deshabilitar esta opción garantiza que el tráfico gestionado por esta interfaz no fluya directamente a la IGW en la VPC.
   - En **Avanzada > Otra información**, amplíe el menú desplegable Perfil de gestión y seleccione el perfil allow_ping que ha creado anteriormente.
   - Haga clic en **ACEPTAR** para guardar la configuración de interfaz.
4. Haga clic en **Compilar** para guardar los cambios.

Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Security Zone
ethernet1/1	Layer3	allow_ping		Dynamic-DHCP Client	default	untrust
ethernet1/2	Layer3	allow_ping		Dynamic-DHCP Client	default	trust

Implementación del cortafuegos VM-Series como una puerta de enlace de la nube (Continuación)

Paso 15 En el cortafuegos VM-Series, cree las reglas NAT de destino y NAT de origen para permitir el tráfico entrante y saliente desde y hacia las aplicaciones implementadas en la VPC.

1. Seleccione **Políticas > NAT**.
2. Cree una regla NAT de destino que envíe el tráfico desde el cortafuegos hasta el servidor web.
   a. Haga clic en **Añadir** e introduzca un Nombre para la regla. Por ejemplo, NAT2WebServer.
   b. En la pestaña **Paquete original**, realice las siguientes selecciones:
      – **Zona de origen**: untrust (donde se origina el tráfico)
      – **Zona de destino**: untrust (la zona para la interfaz del plano de datos del cortafuegos con la que se asocia la EIP para el servidor web).
      – **Dirección de origen**: Cualquiera
      – **Dirección de destino**: 10.0.0.10
      – En la pestaña **Paquete traducido**, seleccione la casilla de verificación Traducción de dirección de destino y establezca la **dirección traducida**: a 10.0.1.62, que es la dirección IP privada del servidor web.
   c. Haga clic en **ACEPTAR**.

			Original Packet						Translated Packet	
	Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
1	NAT2WebServer	none	untrust	untrust	any	any	10.0.0.10	any	none	address: 10.0.1.62

3. Cree una regla NAT de origen para permitir el acceso para el tráfico saliente desde el servidor web a Internet.
   a. Haga clic en **Añadir** e introduzca un Nombre para la regla. Por ejemplo, NAT2External.
   b. En la pestaña **Paquete original**, realice las siguientes selecciones:
      – **Zona de origen**: trust (donde se origina el tráfico)
      – **Zona de destino**: untrust (la zona para la interfaz del plano de datos del cortafuegos con la que se asocia la EIP para el servidor web).
      – **Dirección de origen**: Cualquiera
      – **Dirección de destino**: Cualquiera
   c. En la pestaña **Paquete traducido**, seleccione lo siguiente en la sección Traducción de dirección de origen:
      – **Tipo de traducción**: IP dinámica y puerto
      – **Tipo de dirección**: Dirección traducida
      – **Dirección traducida**: 10.0.0.10 (la interfaz del plano de datos del cortafuegos en la zona no fiable.)

Implementación del cortafuegos VM-Series como una puerta de enlace de la nube (Continuación)

d. Haga clic en **ACEPTAR**.

		Original Packet						Translated Packet	
Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
NAT2WebServer	none	untrust	untrust	any	any	10.0.0.10	any	none	address: 10.0.1.62
NAT2External	none	trust	untrust	any	any	any	any	dynamic-ip-and-port 10.0.0.10	none

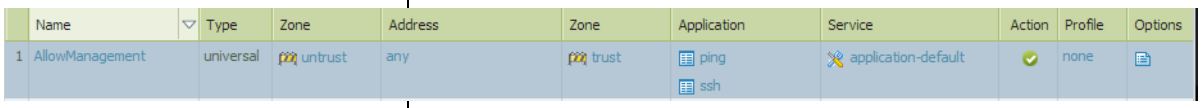
4. Haga clic en **Compilar** para guardar las políticas NAT.

Implementación del cortafuegos VM-Series como una puerta de enlace de la nube (Continuación)

Paso 16 En el cortafuegos VM-Series, cree políticas de seguridad para gestionar el tráfico.

1. Seleccione **Políticas > Seguridad**.

   En este ejemplo, tenemos cuatro reglas: Una regla que permite el acceso a la gestión del tráfico del cortafuegos, una regla que permite el tráfico entrante al servidor web, una tercera regla para permitir el acceso a Internet al servidor web y en la última regla se modifica una regla predeterminada intrazona predefinida para registrar todo el tráfico denegado.
2. Cree una regla para permitir el acceso a la gestión al cortafuegos.
   a. Haga clic en **Añadir** e introduzca un **Nombre** para la regla. Compruebe que el **Tipo de regla** es universal.
   b. En la pestaña **Origen**, seleccione untrust como la **zona de origen**.
   c. En la pestaña **Destino**, añada trust como la **Zona de destino**.
   d. En la pestaña **Aplicaciones**, **añada** ping y ssh.
   e. En la pestaña **Acciones**, establezca **Acción** como Permitir.
   f. Haga clic en **ACEPTAR**.

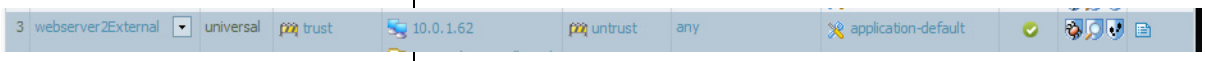


3. Cree una regla para permitir el tráfico entrante al servidor web.
   a. Haga clic en **Añadir** e introduzca un **nombre** para la regla y verifique que el **tipo de regla** es universal.
   b. En la pestaña **Origen**, seleccione untrust como la **zona de origen**.
   c. En la pestaña **Destino**, añada trust como la **Zona de destino**.
   d. En la pestaña **Aplicaciones**, **añada** navegación web.
   e. En la pestaña **Categoría de URL/servicio**, compruebe que el servicio está establecido como predeterminado de la aplicación.
   f. En la pestaña **Acciones**, establezca **Acción** como Permitir.
   g. En la sección Configuración de perfiles de la pestaña **Acciones**, seleccione **Perfiles** y, a continuación, adjunte los perfiles predeterminados para antivirus, antispyware y protección contra vulnerabilidades.
   h. Haga clic en **ACEPTAR**.

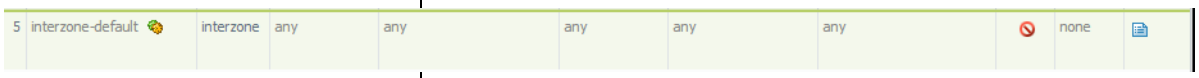
Implementación del cortafuegos VM-Series como una puerta de enlace de la nube (Continuación)

En lugar de introducir una dirección IP estática para el servidor web, use un grupo de direcciones dinámicas. Los grupos de direcciones dinámicas le permiten crear políticas que se adapten automáticamente a los cambios, de modo que no tenga que actualizar la política cuando inicie los servidores web adicionales en la subred. Para obtener más información, consulte Caso de uso: Uso de grupos de direcciones dinámicas para proteger las nuevas instancias de EC2 en la VPC.

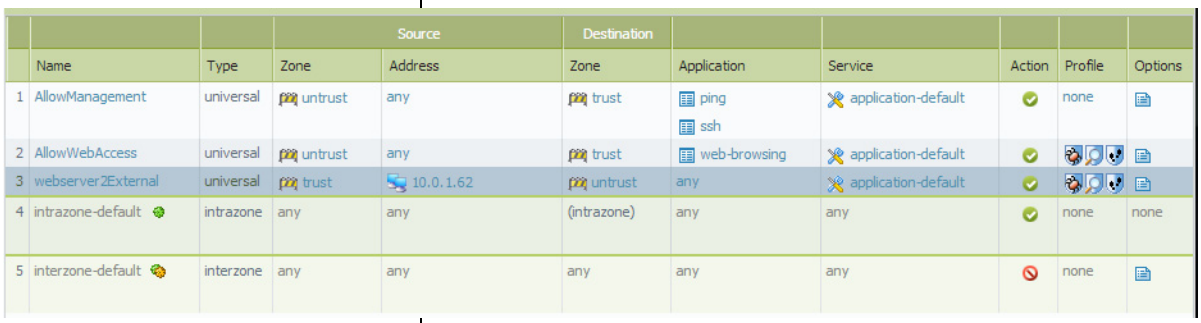
4. Cree una regla para permitir el acceso a Internet al servidor web.
   a. Haga clic en **Añadir** e introduzca un **nombre** para la regla y verifique que el tipo de regla es universal.
   b. En la pestaña **Origen**, seleccione trust como la **zona de origen**.
   c. En la sección Dirección de origen de la pestaña **Origen**, añada 10.0.1.62, la dirección IP del servidor web.
   d. En la pestaña **Destino**, añada untrust como la **Zona de destino**.
   e. En la pestaña **Categoría de URL/servicio**, compruebe que el servicio está establecido como **predeterminado de la aplicación**.
   f. En la pestaña **Acciones**, establezca **Acción** como Permitir.
   g. En la sección Configuración de perfiles de la pestaña **Acciones**, seleccione **Perfiles** y, a continuación, adjunte los perfiles predeterminados para antivirus, antispyware y protección contra vulnerabilidades.
   h. Haga clic en **ACEPTAR**.



5. Modifique la regla predeterminada entre zonas para registrar todo el tráfico denegado. Esta regla predeterminada entre zonas se evalúa cuando no se define explícitamente ninguna otra regla para buscar coincidencias de tráfico en zonas diferentes.
   a. Seleccione la regla **predeterminada entre zonas** y haga clic en **Cancelar**.
   b. En la pestaña **Acciones**, seleccione **Log al finalizar sesión**.
   c. Haga clic en **ACEPTAR**.



6. Revise el conjunto completo de reglas de seguridad definidas en el cortafuegos.



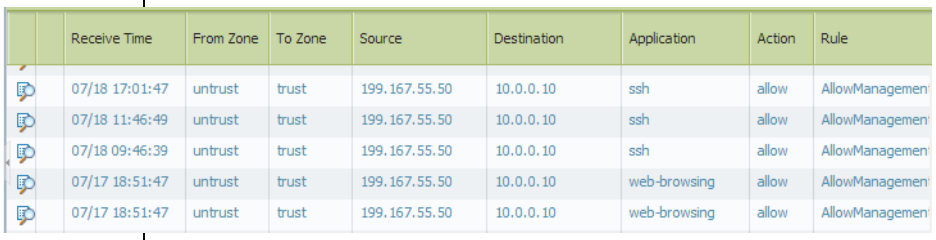
			Source		Destination					
	Name	Type	Zone	Address	Zone	Application	Service	Action	Profile	Options
1	AllowManagement	universal	untrust	any	trust	ping ssh	application-default		none	
2	AllowWebAccess	universal	untrust	any	trust	web-browsing	application-default			
3	webserver2External	universal	trust	10.0.1.62	untrust	any	application-default			
4	intrazone-default	intrazone	any	any	(intrazone)	any	any		none	none
5	interzone-default	interzone	any	any	any	any	any		none	

7. Haga clic en **Compilar** para guardar las políticas.

Implementación del cortafuegos VM-Series como una puerta de enlace de la nube (Continuación)

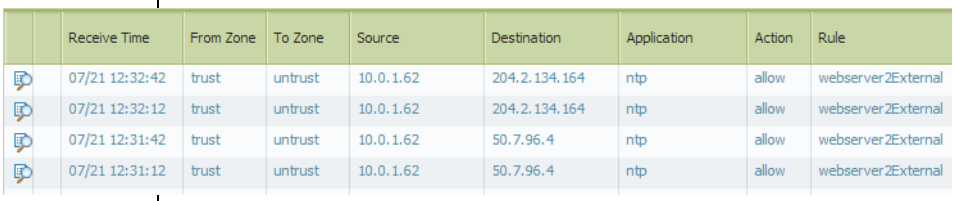
Paso 17 Compruebe que el cortafuegos VM-Series está protegiendo el tráfico.

1. Inicie un navegador web e introduzca la dirección IP del servidor web.
2. Inicie sesión en la interfaz web del cortafuegos VM-Series y compruebe que puede ver los logs de tráfico de las sesiones en **Supervisar > Logs > Tráfico**.
   - Tráfico entrante en el servidor web (llega a la instancia de EC2 en la VPC de AWS):



Receive Time	From Zone	To Zone	Source	Destination	Application	Action	Rule
07/18 17:01:47	untrust	trust	199.167.55.50	10.0.0.10	ssh	allow	AllowManagemen
07/18 11:46:49	untrust	trust	199.167.55.50	10.0.0.10	ssh	allow	AllowManagemen
07/18 09:46:39	untrust	trust	199.167.55.50	10.0.0.10	ssh	allow	AllowManagemen
07/17 18:51:47	untrust	trust	199.167.55.50	10.0.0.10	web-browsing	allow	AllowManagemen
07/17 18:51:47	untrust	trust	199.167.55.50	10.0.0.10	web-browsing	allow	AllowManagemen

   - Tráfico saliente del servidor web (instancia de EC2 en la VPC de AWS):



Receive Time	From Zone	To Zone	Source	Destination	Application	Action	Rule
07/21 12:32:42	trust	untrust	10.0.1.62	204.2.134.164	ntp	allow	webserver2External
07/21 12:32:12	trust	untrust	10.0.1.62	204.2.134.164	ntp	allow	webserver2External
07/21 12:31:42	trust	untrust	10.0.1.62	50.7.96.4	ntp	allow	webserver2External
07/21 12:31:12	trust	untrust	10.0.1.62	50.7.96.4	ntp	allow	webserver2External

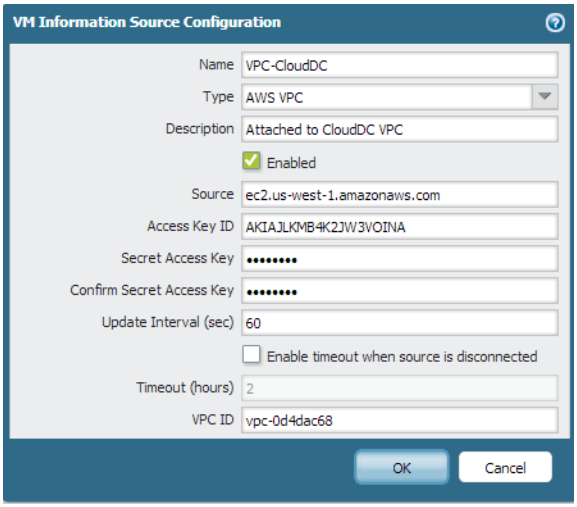
Ha implementado correctamente el cortafuegos VM-Series como una puerta de enlace de la nube.

Caso de uso: Uso de grupos de direcciones dinámicas para proteger las nuevas instancias de EC2 en la VPC

En un entorno dinámico como la VPC de AWS, donde inicia las nuevas instancias de EC2 bajo demanda, la carga de trabajo administrativa de la gestión de la política de seguridad puede ser excesiva. El uso de grupos de direcciones dinámicas en la política de seguridad aporta agilidad y evita las interrupciones en los servicios o brechas en la protección.

En este ejemplo, se ilustra cómo puede supervisar la VPC y usar grupos de direcciones dinámicas en la política de seguridad para detectar y proteger instancias de EC2. Al iniciar las instancias de EC2, el grupo de direcciones dinámicas coteja las direcciones IP de todas las instancias que coinciden con los criterios definidos para la pertenencia al grupo y, a continuación, se aplica la política de seguridad del grupo. La política de seguridad en este ejemplo permite el acceso a Internet a todos los miembros del grupo.

Este flujo de trabajo en la siguiente sección asume que ha creado la VPC de AWS e implementado el cortafuegos VM-Series y algunas aplicaciones en instancias EC2. Para obtener instrucciones sobre la configuración de la VPC para VM-Series, consulte Caso de uso: Protección de las instancias de EC2 en AWS Cloud.

Uso de grupos de direcciones dinámicas en políticas	
Paso 1 Configure el cortafuegos para supervisar la VPC.	1. Seleccione **Dispositivo > Orígenes de información de VM**. 2. Haga clic en **Añadir** y especifique la siguiente información: a. Un **nombre** para identificar la VPC que quiere supervisar. Por ejemplo, VPC-CloudDC. b. Establezca el **tipo** como VPC de AWS. c. En **Origen**, introduzca la URI de la VPC. La sintaxis es: ec2.<*su_región*>.amazonaws.com d. Añada las credenciales necesarias para que el cortafuegos firme digitalmente las llamadas de API realizadas por los servicios de AWS. Necesitará lo siguiente: – **ID de clave de acceso**: Introduzca la cadena de texto alfanumérico que identifica de forma exclusiva al usuario propietario o con autorización de acceso a la cuenta de AWS. – **Clave de acceso secreta**: Introduzca la contraseña y confirme la entrada. e. (Opcional) Modifique el **intervalo de actualización** a un valor entre 5-600 segundos. De manera predeterminada, el cortafuegos sondea cada 5 segundos. Las llamadas de API se ponen en cola y recuperan cada 60 segundos, de modo que las actualizaciones pueden tardar hasta 60 segundos, más el intervalo de sondeo configurado.  f. Introduzca el **ID de la VPC** que se muestra en el panel VPC en la consola de gestión de AWS. g. Haga clic en **ACEPTAR** y seleccione **Confirmar** los cambios. h. Compruebe que el **Estado** de conexión aparece como conectado.

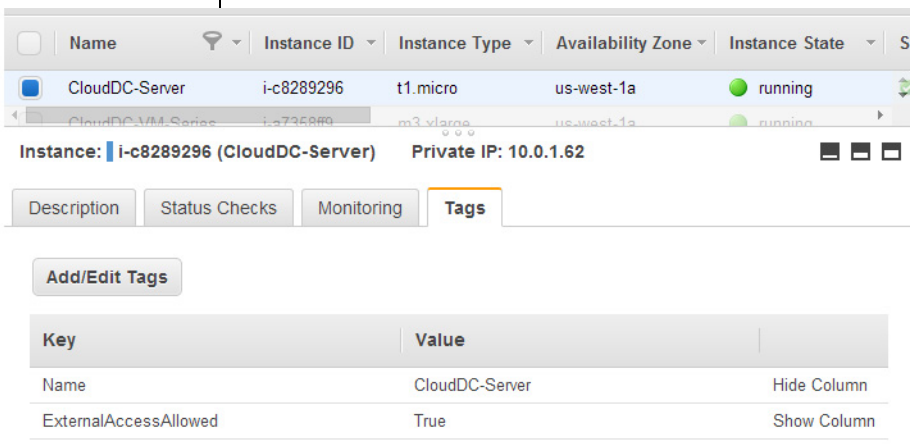
Uso de grupos de direcciones dinámicas en políticas (Continuación)

Paso 2 Etiquete las instancias de EC2 en la VPC.

Puede consultar en Lista de atributos supervisados en la VPC de AWS una lista de etiquetas que el cortafuegos VM-Series puede supervisar.

Una etiqueta es un par nombre-valor. Puede etiquetar las instancias de EC2 en el panel EC2 de la consola de gestión de AWS o usando la API de AWS o la CLI de AWS.

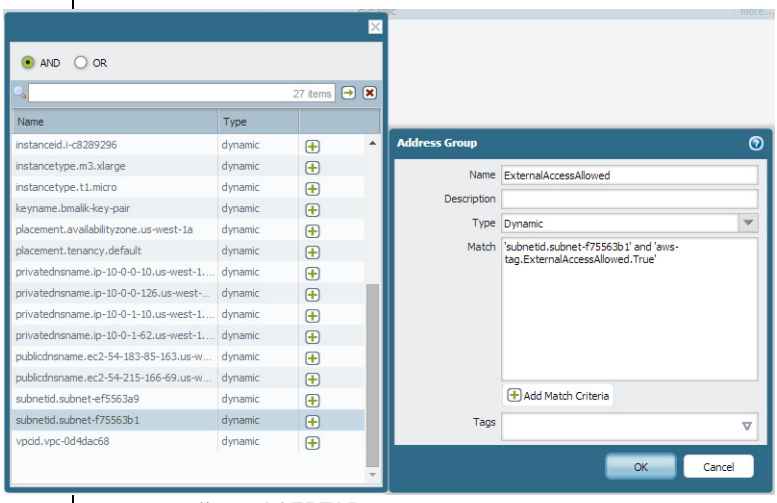
En este ejemplo, usamos el panel EC2 para añadir la etiqueta:



Paso 3 Cree un grupo de direcciones dinámicas en el cortafuegos.

Vea el tutorial para obtener información detallada de la función.

3. Seleccione **Objeto > Grupos de direcciones**.
4. Haga clic en **Añadir** e introduzca un **Nombre** y una **Descripción** del grupo de direcciones.
5. Defina el **Tipo** como **Dinámico**.
6. Defina los criterios de coincidencia.
   a. Haga clic en **Añadir criterios de coincidencia** y seleccione el operador **Y**.
   b. Seleccione los atributos de filtrado o búsqueda de coincidencias. En este ejemplo, se selecciona la etiqueta ExternalAccessAllowed que acaba de crear y el ID de subred de la subred privada de la VPC.



7. Haga clic en **ACEPTAR**.
8. Haga clic en **Compilar**.

Uso de grupos de direcciones dinámicas en políticas (Continuación)

Paso 4 Uso del grupo de direcciones dinámicas en una política de seguridad.

Para crear una regla que permita el acceso a Internet a cualquier servidor web que pertenezca al grupo de direcciones dinámicas llamado ExternalServerAccess.

1. Seleccione **Políticas > Seguridad**.
2. Haga clic en **Añadir** e introduzca un **nombre** para la regla y verifique que el **tipo de regla** es universal.
3. En la pestaña **Origen**, seleccione trust como la **zona de origen**.
4. En la sección Dirección de origen de la pestaña **Origen**, **añada** el grupo ExternalServerAccess que acaba de crear.
5. En la pestaña **Destino**, añada untrust como la **Zona de destino**.
6. En la pestaña **Categoría de URL/servicio**, compruebe que el servicio está establecido como **predeterminado de la aplicación**.
7. En la pestaña **Acciones**, establezca **Acción** como Permitir.
8. En la sección Configuración de perfiles de la pestaña **Acciones**, seleccione **Perfiles** y, a continuación, adjunte los perfiles predeterminados para antivirus, antispyware y protección contra vulnerabilidades.
9. Haga clic en **ACEPTAR**.

			Source		Destination					
	Name	Type	Zone	Address	Zone	Application	Service	Action	Profile	Options
2	AllowWebAccess	universal	untrust	any	trust	web-browsing	application-default			
3	webserver2External	universal	trust	ExternalAccessAllowed	untrust	any	application-default			

10. Haga clic en **Compilar**.

Paso 5 Comprobar que los miembros del grupo de direcciones dinámicas se han añadido al cortafuegos.

La política entra en vigor para todas las direcciones IP que pertenecen a este grupo de direcciones y se muestra aquí.

1. Seleccione **Políticas > Seguridad** y seleccione la regla.
2. Seleccione la flecha desplegable junto al vínculo del grupo de direcciones y seleccione **Inspeccionar**. También puede comprobar si los criterios de coincidencia son precisos.
3. Haga clic en el vínculo **más** y compruebe que se muestra la lista de direcciones IP registradas.

Lista de atributos supervisados en la VPC de AWS

Los siguientes atributos (o nombres de etiquetas) están disponibles como criterios de coincidencias para grupos de direcciones dinámicas.

Atributo	Formato
Arquitectura	Architecture.<cadena Architecture>
Sistema operativo invitado	GuestOS.<nombre de sistema operativo invitado>
ID de imagen	ImageId.<cadena ImageId>
ID de instancia	InstanceId.<cadena InstanceId>
Estado de instancia	InstanceState.<estado de instancia>
Tipo de instancia	InstanceType.<tipo de instancia>
Nombre de clave	KeyName.<cadena KeyName>
Colocación: arrendamiento, nombre de grupo, disponibilidad	Placement.Tenancy.<cadena> Placement.GroupName.<cadena> Placement.AvailabilityZone.<cadena>
Nombre de DNS privado	PrivateDnsName.<Nombre de DNS privado>
Nombre de DNS público	PublicDnsName.<Nombre de DNS público>
ID de subred	SubnetID.<cadena subnetID>
Etiqueta (clave, valor)	aws-tag.<clave>.<valor> Cada instancia admite 5 de estas etiquetas como máximo
ID de VPC	VpcId.<cadena VpcId>

Caso de uso: Cortafuegos VM-Series como puertas de enlace de GlobalProtect en AWS

La protección de los usuarios de dispositivos móviles ante amenazas y aplicaciones de riesgo suele consistir en una compleja combinación de adquisición y configuración de la seguridad e infraestructura de TI, aseguramiento del ancho de banda y los requisitos de tiempo de actividad en todo el mundo, todo ello sin salirse del presupuesto.

El cortafuegos VM-Series en AWS combina la seguridad y la logística de TI necesarias para proteger de forma consistente y fiable los dispositivos móviles de usuarios en regiones donde no está presente. Al implementar un cortafuegos VM-Series en la nube AWS, puede implementar rápida y fácilmente GlobalProtect en cualquier región sin el gasto o la logística de TI que suelen ser necesarias para establecer esta infraestructura usando sus propios recursos.

Para reducir al mínimo la latencia, seleccione las regiones de AWS más cercanas a sus usuarios, implemente los cortafuegos VM-Series en las instancias de EC2 y configure los cortafuegos como puertas de enlace de GlobalProtect. Con esta solución, las puertas de enlace de GlobalProtect en la nube de AWS aplican políticas de seguridad para el tráfico de Internet, de modo que no haya que desviarlo por la red corporativa. Asimismo, para el acceso a recursos en la red corporativa, el cortafuegos VM-Series en AWS aprovecha la funcionalidad LSVPN para establecer túneles de IPSec de nuevo en el cortafuegos de la red corporativa.

Para una implementación sencilla y una gestión centralizada de esta, use Panorama para configurar los componentes de GlobalProtect usados en esta solución. De manera opcional, para garantizar el uso seguro de los dispositivos móviles (smartphones y tablets) en su red, use el gestor de seguridad móvil para configurar y gestionar dispositivos móviles.

Componentes de la infraestructura de GlobalProtect

Para bloquear las aplicaciones inseguras y proteger a los usuarios móviles contra el software malintencionado, debe configurar la infraestructura de GlobalProtect que incluye el portal de GlobalProtect, la puerta de enlace de GlobalProtect y la aplicación GlobalProtect. Asimismo, para acceder a los recursos corporativos, debe configurar una conexión de VPN de IPSec entre los cortafuegos VM-Series en AWS y el cortafuegos de la sede corporativa mediante LSVPN (una implementación de VPN de concentrador y radio).

- El agente o la aplicación de GlobalProtect se instala en cada sistema de usuario final que se use para acceder a aplicaciones o recursos corporativos. El agente se conecta primero al portal para obtener información sobre las puertas de enlace y, a continuación, establece una conexión de VPN segura con la puerta de enlace de GlobalProtect. La conexión de VPN entre el sistema de usuario final y la puerta de enlace garantiza la privacidad de los datos.
- El portal de GlobalProtect proporciona las funciones de gestión para la infraestructura de GlobalProtect. Todos los sistemas de usuarios finales reciben información de configuración desde el portal, incluida la información sobre las puertas de enlace disponibles, así como certificados de cliente que pueden ser necesarios para conectarse a las puertas de enlace de GlobalProtect. En este caso de uso, el portal de GlobalProtect es un cortafuegos basado en hardware que se implementa en la sede corporativa.
- La puerta de enlace de GlobalProtect y el forzaje de políticas basadas en aplicaciones, usuarios, contenido, dispositivos y estado de dispositivos. En este caso de uso, los cortafuegos VM-Series en AWS funcionan como las puertas de enlace de GlobalProtect. La puerta de enlace de GlobalProtect analiza posible software malintencionado y otras amenazas en las solicitudes de los usuarios, y si la política lo permite, envía la solicitud a Internet o a la red corporativa a través del túnel de IPSec (a la puerta de enlace de LSVPN).
- Para LSVPN, debe configurar el portal de GlobalProtect, la puerta de enlace de GlobalProtect para LSVPN (concentrador) y los satélites de GlobalProtect (radios).

  En este caso de uso, el cortafuegos basado en hardware en la oficina corporativa se implementa como el portal de GlobalProtect y la puerta de enlace de LSVPN. Los cortafuegos VM-Series en AWS están configurados para funcionar como satélites de GlobalProtect. Los satélites y la puerta de enlace de GlobalProtect están configurados para establecer un túnel de IPSec que finaliza en la puerta de enlace. Cuando un usuario de un dispositivo móvil solicita una aplicación o recurso alojado en la red corporativa, el cortafuegos VM-Series enruta la solicitud a través del túnel de IPSec.

Implementación de puertas de enlace de GlobalProtect en AWS

Para proteger a los usuarios de dispositivos móviles, además de implementar y configurar las puertas de enlace de GlobalProtect en AWS, necesita configurar el resto de componentes necesarios para esta solución integrada. La siguiente tabla enumera el flujo de trabajo recomendado.

Implementación de GlobalProtect en AWS	
• Implementación de cortafuegos VM-Series en AWS	Consulte Implementación del cortafuegos VM-Series en AWS.

Implementación de GlobalProtect en AWS (Continuación)	
• Configure el cortafuegos en la sede corporativa. En este caso de uso, el cortafuegos está configurado como el portal de GlobalProtect y la puerta de enlace de LSVPN.	• Configure el portal de GlobalProtect. • Configure el portal de GlobalProtect para LSVPN. • Configure el portal para la autenticación de satélites de LSVPN. • Configure la puerta de enlace de GlobalProtect para LSVPN.
• Configure una plantilla en Panorama para la configuración de los cortafuegos VM-Series en AWS como puertas de enlace de GlobalProtect y satélites de LSVPN. Para gestionar fácilmente esta implementación distribuida, use Panorama para configurar los cortafuegos en AWS.	• Cree plantillas en Panorama. A continuación, use los siguientes enlaces para definir la configuración en las plantillas. • Configure el cortafuegos como una puerta de enlace de GlobalProtect. • Prepare el satélite para unirse a la LSVPN.
• Cree grupos de dispositivos en Panorama para definir las políticas de acceso a la red y las reglas de acceso a Internet y aplíquelas a los cortafuegos en AWS.	Consulte Creación de grupos de dispositivos.
• Aplique las plantillas y los grupos de dispositivos a los cortafuegos VM-Series en AWS y compruebe que los cortafuegos están correctamente configurados.	
• Implementación del software de cliente de GlobalProtect.	Cada sistema de usuario final necesita el agente o aplicación de GlobalProtect para conectarse a la puerta de enlace de GlobalProtect. Consulte Implementación del software de cliente de GlobalProtect.
• (Opcional) Configure el gestor de seguridad móvil de GlobalProtect El gestor de seguridad móvil le permite configurar y gestionar dispositivos móviles (smartphones y tablets) para su uso con aplicaciones corporativas.	Consulte Configuración del gestor de seguridad móvil.

Configuración del cortafuegos VM-Series en KVM

Kernel-based Virtual Machine (KVM) es un módulo de virtualización de código abierto para servidores que ejecutan distribuciones Linux. El cortafuegos VM-Series se puede implementar en un servidor Linux que ejecute el hipervisor KVM.

En esta guía se asume que ya utiliza infraestructura de TI basada en Linux y dispone de lo necesario para el uso de herramientas de Linux y herramientas de Linux. Las instrucciones sólo hacen referencia a la implementación del cortafuegos VM-Series en KVM.

- VM-Series en KVM: Especificaciones y requisitos previos
- Implementaciones compatibles con KVM
- Instalación del cortafuegos VM-Series en KVM

VM-Series en KVM: Especificaciones y requisitos previos

Requisitos del sistema

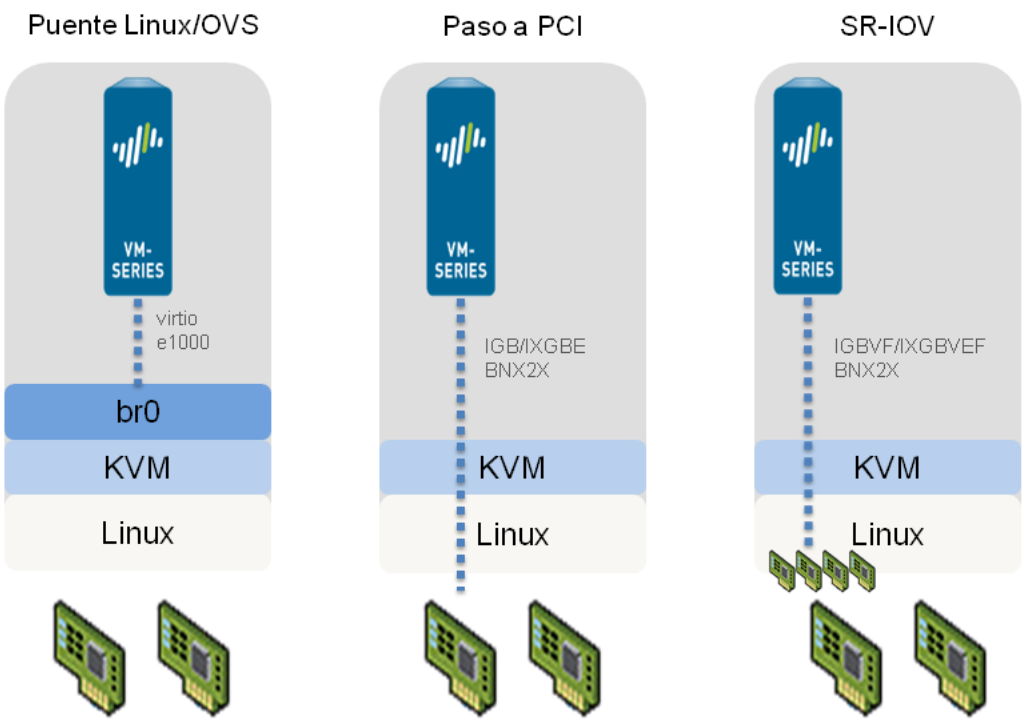
Requisitos	Descripción

Recursos de hardware	• vCPU: 2, 4, 8
	• Memoria: 4 GB; 5 GB para VM-1000-HV
	• Disco: 40 GB
	  • Tipos de discos compatibles: Virtio y SCSI para obtener el mejor rendimiento; IDE
	  • Controladores de disco: virtio, virt-scsi, IDE
	• Conjunto de chips Intel-VT o AMD-V compatible con la virtualización asistida por hardware

Versiones de software	• Ubuntu: 12.04 LTS • CentOS/ RedHat Enterprise Linux: 6.5 • Open vSwitch: 1.9.3 con modo de compatibilidad de puente

Interfaces de red: Tarjetas de interfaz de red y puentes de software	VM-Series en KVM admite un máximo de 25 interfaces: 1 interfaz de gestión y un máximo de 24 interfaces de red para tráfico de datos.
	VM-Series implementado en KVM admite conmutadores virtuales basados en software como el puente Linux o el puente Open vSwitch, así como conectividad directa al envío PCI o a un adaptador compatible con SR-IOV.
	• En el puente Linux y OVS, son compatibles los controladores e1000 y virtio; no es compatible el controlador predeterminado rtl8139.
	• En cuanto a la compatibilidad de envío PCI/SR-IOV, se han probado las siguientes tarjetas de red para el cortafuegos VM-Series :
	  – Tarjeta de red 1G basada en Intel 82576: Compatibilidad con SR-IOV en todas las distribuciones de Linux compatibles; compatibilidad con envío PCI en todas excepto Ubuntu 12.04 LTS.
	  – Tarjeta de red 10G basada en Intel 82599: Compatibilidad con SR-IOV en todas las distribuciones de Linux compatibles; compatibilidad con envío PCI en todas excepto Ubuntu 12.04 LTS.
	  – Tarjeta de red 10G basada en Broadcom 57112 y 578xx: Compatibilidad con SR-IOV en todas las distribuciones de Linux compatibles; no compatible con envío PCI.
	  • Controladores: igb; ixgbe; bnx2x
	  • Controladores: igbvf; ixgbevf; bnx2x
	 Las interfaces compatibles con SR-IOV asignadas al cortafuegos VM-Series deben configurarse como interfaces de capa 3 o como interfaces HA.

Opciones para adjuntar el VM-Series en la red



- Con un puente Linux u OVS, el tráfico de datos usa el puente de software para conectar invitados en el mismo host. Para la conectividad externa, el tráfico de datos usa la interfaz física a la que se ha adjuntado el puente.
- Con el envío PCI, el tráfico de datos pasa directamente entre el invitado y la interfaz física a la que está adjuntada. Cuando la interfaz se adjunta a un invitado, no está disponible para el host o para otros invitados en el host.
- Con SR-IOV, el tráfico de datos pasa directamente entre el invitado y la función virtual a la que está adjuntada.

Requisitos previos para VM-Series en KVM

Antes de instalar el cortafuegos VM-Series en el servidor Linux, consulte las siguientes secciones:

▲ Preparación del servidor Linux

▲ Preparación de la implementación del cortafuegos VM-Series

Preparación del servidor Linux

- Compruebe la versión de distribución de Linux. Para ver una lista de las versiones compatibles, consulte Requisitos del sistema.
- Compruebe que ha instalado y configurado las herramientas y paquetes de KVM necesarios para crear y gestionar máquinas virtuales, como Libvirt.
- Si quiere usar un controlador de disco SCSI para acceder al disco en el que el cortafuegos VM-Series almacena los datos, debe usar virsh para adjuntar el controlador virtio-scsi al cortafuegos VM-Series. A continuación, puede modificar la plantilla XML del cortafuegos VM-Series para habilitar el uso del controlador virtio-scsi. Para obtener instrucciones, consulte Habilitación del uso de un controlador SCSI.

  KVM en Ubuntu 12.04 no admite el controlador virtio-scsi.

- Compruebe que ha configurado la infraestructura de red para enviar el tráfico entre los invitados y el cortafuegos VM-Series y para la conectividad con un servidor externo de Internet. El cortafuegos VM-Series puede conectar usando un puente Linux, Open vSwitch, envío PCI o una tarjeta de red compatible con SR-IOV.
  - Compruebe que los enlaces de todas las interfaces que pretende usar estén en estado activo; en ocasiones, puede que tenga que activarlas de forma manual.
  - Compruebe el PCI ID de todas las interfaces. Para exportar la lista, use el comando: `Virsh nodedev-list –tree`
  - Si usa un puente Linux u OVS, compruebe que tiene configurados los puentes necesarios para enviar o recibir tráfico desde y hacia el cortafuegos. De lo contrario, cree puentes y compruebe que estén activos antes de iniciar la instalación del cortafuegos.
  - Si usa envío PCI o SR-IOV, compruebe que las extensiones de virtualización (VT-d/IOMMU) están habilitadas en la BIOS. Por ejemplo, para habilitar IOMMU, `intel_iommu=on` debe estar definido en `/etc/grub.conf`. Consulte las instrucciones en la documentación suministrada por el proveedor del sistema.
  - Si usa envío PCI, asegúrese de que el cortafuegos VM-Series tiene acceso exclusivo a las interfaces que tiene pensado adjuntarle.

    Para permitir el acceso exclusivo, debe desasociar las interfaces del servidor Linux; consulte las instrucciones en la documentación suministrada por el proveedor de la tarjeta de red.

    Para desasociar manualmente las interfaces del servidor, use el comando:

    `Virsh nodedev-detach <pci id de la interfaz>, por ejemplo, pci_0000_07_10_0`

    En algunos casos, en `/etc/libvirt/qemu.conf`, tal vez deba quitar la marca de comentario `relaxed_acs_check = 1`.
  - Si usa SR-IOV, compruebe que la capacidad de funcionamiento virtual esté habilitada para el puerto en el que tiene pensado usar la tarjeta de red. Con SR-IOV, un único puerto Ethernet (función física) se puede dividir en varias funciones virtuales múltiples. Un invitado se puede asignar a una o más funciones virtuales.

Para habilitar funciones virtuales, necesita:

1. Crear un nuevo archivo en esta ubicación: /etc/modprobe.d/

2. Modificar el archivo usando el editor de vi para que las funciones sean constantes: vim /etc/modprobe.d/igb.conf

3. Habilitar el número de funciones virtuales requeridas: options igb max_vfs=4

Después de guardar los cambios y reiniciar el servidor Linux, cada interfaz (o función física) de este ejemplo tendrá 4 funciones virtuales.

Consulte los detalles sobre el número concreto de funciones virtuales y las instrucciones para habilitarlas en la documentación suministrada por el proveedor de red.

Preparación de la implementación del cortafuegos VM-Series

- Adquiera el modelo VM-Series y registre el código de autorización en el portal de asistencia de Palo Alto Networks. Consulte Creación de una cuenta de asistencia técnica y Registro del cortafuegos VM-Series.
- Obtenga la imagen qcow2 y guárdela en el servidor Linux. Se recomienda copiar la imagen en la carpeta: `/var/lib/libvirt/qemu/images`

  Si tiene pensado implementar más de una instancia del cortafuegos VM-Series, haga el número necesario de copias de la imagen. Dado que cada instancia del cortafuegos VM-Series mantiene un vínculo con la imagen .qcow2 que se usó para la implementación del cortafuegos, para evitar problemas de daños de los datos, compruebe que cada imagen sea independiente y la use una única instancia del cortafuegos.

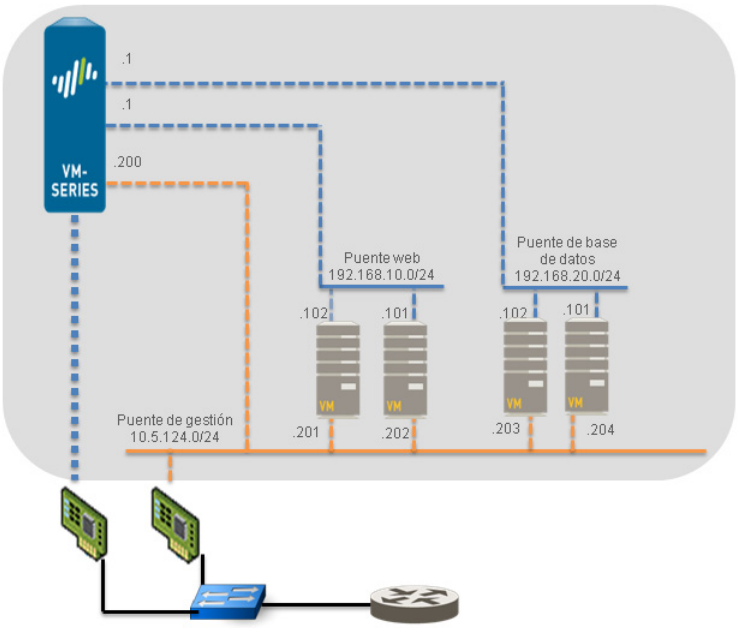
Implementaciones compatibles con KVM

Puede implementar una única instancia del cortafuegos VM-Series por host Linux (inquilino único) o instancias múltiples de cortafuegos VM-Series en un host Linux. El cortafuegos VM-Series se puede implementar con interfaces virtual wire, de capa 2 o de capa 3. Si tiene previsto usar interfaces compatibles con SR-IOV en el cortafuegos VM-Series, sólo puede configurar las interfaces como interfaces de capa 3.

- Protección del tráfico en un host único
- Protección del tráfico a través de hosts Linux

Protección del tráfico en un host único

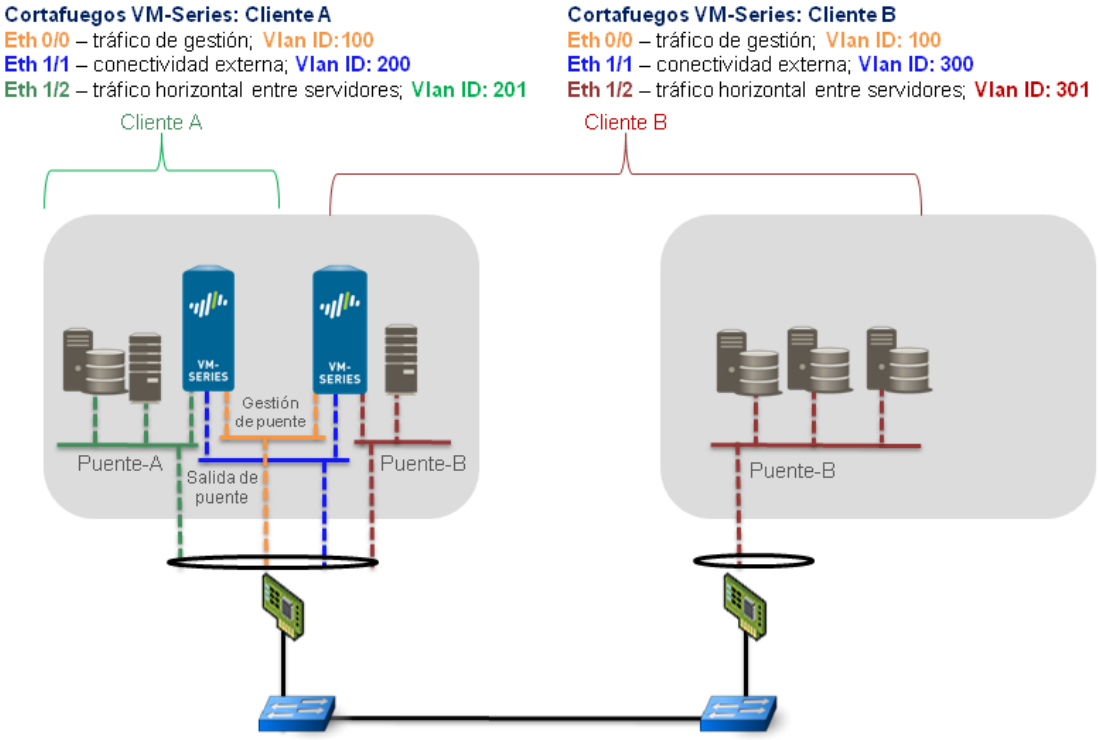
Para proteger el tráfico de dispositivo a dispositivo en invitados de un servidor Linux, el cortafuegos VM-Series se puede implementar con interfaces virtual wire, capa 2 o capa 3. La siguiente ilustración muestra el cortafuegos con interfaces de capa 3, donde el cortafuegos y otros invitados en el servidor están conectados mediante el uso de puentes Linux. En esta implementación, todo el tráfico entre los servidores web y los servidores de bases de datos se enruta a través de cortafuegos; el tráfico que atraviesa sólo los servidores de bases de datos o sólo los servidores web es procesado por el puente y no se enruta a través del cortafuegos.



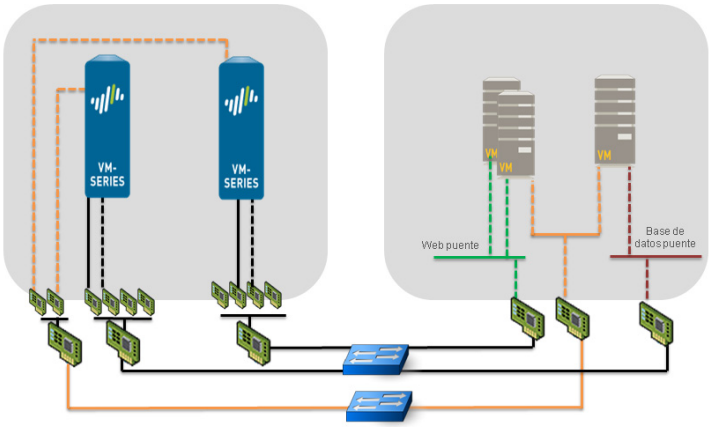
Protección del tráfico a través de hosts Linux

Para proteger sus cargas de trabajo, se puede implementar más de una instancia de cortafuegos VM-Series en un host Linux. Si, por ejemplo, quiere aislar el tráfico para departamentos o clientes separados, puede usar etiquetas VLAN.

para aislar lógicamente el tráfico de red y enrutarlo al cortafuegos VM-Series apropiado. En el siguiente ejemplo, un host Linux aloja el cortafuegos VM-Series para dos clientes, Cliente A y Cliente B, y la carga de trabajo para el Cliente B se reparte a través de dos servidores. Para aislar el tráfico y dirigirlo al cortafuegos VM-Series configurado para cada cliente, se usan VLAN.



En otra variación de esta implementación, se implementa un par de cortafuegos VM-Series en una configuración de alta disponibilidad. Los cortafuegos VM-Series en la siguiente ilustración se implementan en un servidor Linux con adaptadores compatibles SR-IOV. Con SR-IOV, un único puerto Ethernet (función física) se puede dividir en varias funciones virtuales múltiples. Cada función virtual adjunta al cortafuegos VM-Series se configura como una interfaz de capa 3. El peer activo en el par HA protege el tráfico que se enruta hacia él desde invitados que están implementados en un servidor Linux diferente.



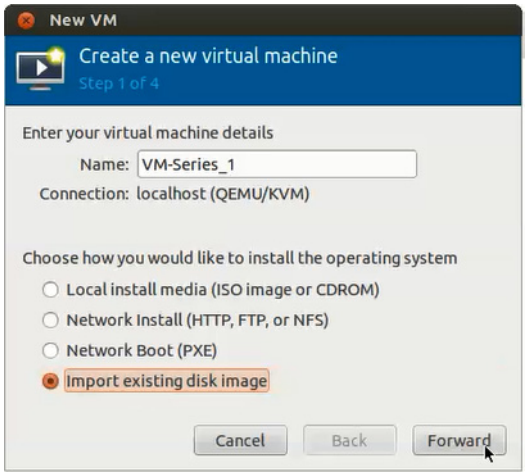
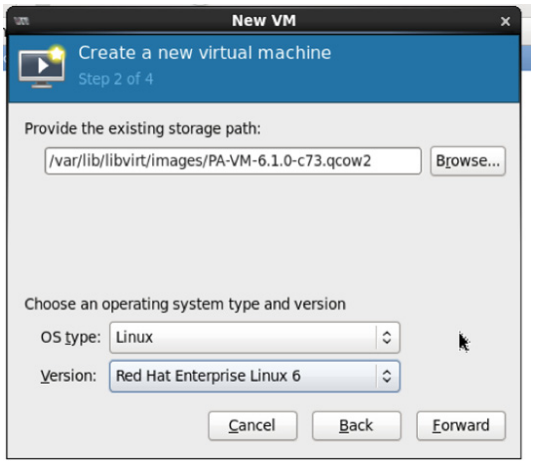
Instalación del cortafuegos VM-Series en KVM

La API libvirt que se usa para gestionar KVM incluye varias herramientas que le permiten crear y gestionar máquinas virtuales. Para instalar el cortafuegos VM-Series en KVM, puede seguir uno de estos métodos:

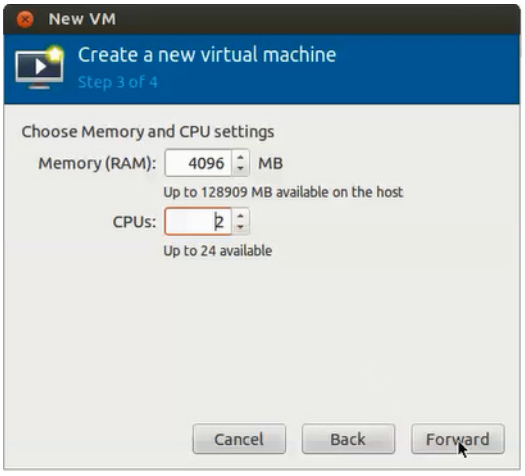
- Cree manualmente la definición XML del cortafuegos VM-Series y, a continuación, use virsh para importar la definición. Virsh es la herramienta más potente que permite la administración completa de la máquina virtual.
- Use virt-install para crear la definición del cortafuegos VM-Series e instálelo.
- Use la interfaz de usuario de escritorio llamada virt-manager; virt-manager ofrece un cómodo asistente para ayudarle a través del proceso de instalación.

El siguiente procedimiento usa virt-manager para instalar el cortafuegos VM-Series en un servidor que ejecute KVM en RHEL; las instrucciones para usar virsh o virt-install no se incluyen en este documento.

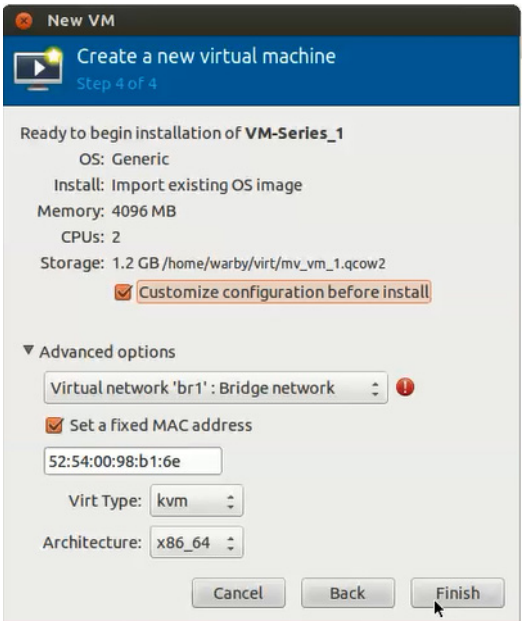
Si está implementando varios cortafuegos VM-Series y quiere automatizar la configuración inicial en el cortafuegos, consulte Uso de un archivo ISO para implementar el cortafuegos VM-Series.

Instalación de VM-Series en KVM	
Paso 1 Instale el cortafuegos VM-Series.	1. En Virt-manager, seleccione **Crear una nueva máquina virtual**. 2. Añada un **nombre** descriptivo para el cortafuegos VM-Series.  3. Seleccione **Importar imagen de disco existente**, navegue hasta la imagen y establezca el **tipo de sistema operativo**: Linux y **Versión**: Red Hat Enterprise Linux 6. Si lo prefiere, puede dejar Tipo de sistema operativo y Versión como Genérico.  4. Establezca la **Memoria** en 4096 MB; o 5120 MB, si ha adquirido la licencia de VM-1000-HV. 5. Establezca **CPU** en 2, 4 u 8.

Instalación de VM-Series en KVM (Continuación)



6. Seleccione **Personalizar configuración antes de la instalación**.
7. En Opciones avanzadas, seleccione el puente para la interfaz de gestión y acepte la configuración predeterminada.

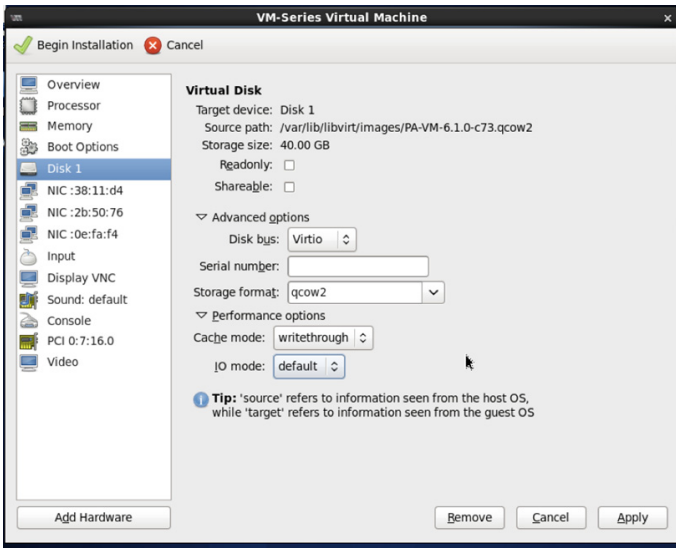


Instalación de VM-Series en KVM (Continuación)

8. Para modificar la configuración de disco:
   a. Seleccione **Disco**, expanda las opciones avanzadas y seleccione **Formato de almacenamiento**: qcow2; **Bus de disco**: Virtio o IDE, en función de su configuración.

      Si quiere usar un bus de disco SCSI, consulte Habilitación del uso de un controlador SCSI.

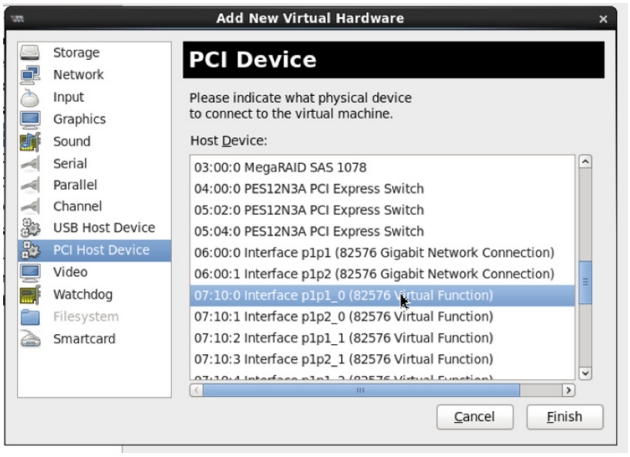
   b. Expanda Opciones de rendimiento y configure **Modo de caché** como WriteThrough. Esta configuración mejora el tiempo de instalación y la velocidad de ejecución en el cortafuegos VM-Series.



Instalación de VM-Series en KVM (Continuación)

9. Para añadir adaptadores de red a las interfaces de datos:
   a. Seleccione **Añadir hardware** > **Red** si está usando un puente de software como un puente Linux u Open vSwitch.
      - En **Dispositivo Host**, introduzca el nombre del puente o selecciónelo de la lista desplegable.
      - Para especificar el controlador, establezca **Modelo de dispositivo** en e-1000 o virtio. Estos son los únicos tipos de interfaces virtuales compatibles.

   b. Seleccione **Añadir hardware** > **Dispositivo host PCI** para Envío PCI o un dispositivo compatible con SR-IOV.



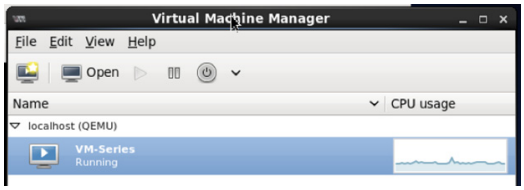
      - En la lista **Dispositivo host**, seleccione la interfaz en la tarjeta o la función virtual.

   c. Haga clic en **Aplicar** o **Finalizar**.

10. Haga clic en Iniciar instalación

.

Instalación de VM-Series en KVM (Continuación)

De manera predeterminada, la plantilla XML del cortafuegos VM-Series se crea y almacena en `etc/libvirt/qemu`.	11. Espere entre 5 y 7 minutos a que se complete la instalación. 
Paso 2 Defina la configuración de acceso a la red para la interfaz de gestión.	1. Abra una conexión a la consola. 2. Inicie el cortafuegos con nombre de usuario/contraseña: admin/admin. 3. Introduzca el siguiente comando: `set deviceconfig system ip-address <IP-cortafuegos> netmask <máscara de red> default-gateway <IP-puerta de enlace> dns-setting servers primary <IP-DNS>` donde <IP-cortafuegos> es la dirección IP que quiere asignar a la interfaz de gestión, <máscara de red> es la máscara de subred, <IP-puerta de enlace> es la dirección IP de la puerta de enlace de la red e <IP-DNS> es la dirección IP del servidor DNS.
Paso 3 Verifique los puertos del host que se asignarán a la interfaz en el cortafuegos VM-Series. Para comprobar el orden de las interfaces en el host Linux, consulte Comprobación de PCI-ID para la ordenación de interfaces de red en el cortafuegos VM-Series.	Para asegurarse de que el tráfico es gestionado por la interfaz correcta, use el siguiente comando para identificar qué puertos en el host se asignan a los puertos en el cortafuegos VM-Series. `admin@PAN-VM>` **`debug show vm-series interfaces all`** Phoenix_interface Base-OS_port Base-OS_MAC PCI-ID mgt eth0 52:54:00:d7:91:52 0000:00:03.0 Ethernet1/1 eth1 52:54:00:fe:8c:80 0000:00:06.0 Ethernet1/2 eth2 0e:c6:6b:b4:72:06 0000:00:07.0 Ethernet1/3 eth3 06:1b:a5:7e:a5:78 0000:00:08.0 Ethernet1/4 eth4 26:a9:26:54:27:a1 0000:00:09.0 Ethernet1/5 eth5 52:54:00:f4:62:13 0000:00:10.0
Paso 4 Acceda a la interfaz web del cortafuegos VM-Series, configure las interfaces y defina las reglas de seguridad y las reglas NAT para habilitar de forma segura las aplicaciones que quiere proteger.	Consulte la Guía del administrador de PAN-OS.

Habilitación del uso de un controlador SCSI

Si quiere que el cortafuegos VM-Series use el tipo de bus de disco SCSI para acceder al disco virtual, use las siguientes instrucciones para adjuntar el controlador virtio scsi al cortafuegos y, a continuación, habilite el uso del controlador virtio-scsi.

KVM en Ubuntu 12.04 no es compatible con el controlador virtio-scsi; el controlador virtio-scsi sólo se puede habilitar en el cortafuegos VM-Series que se ejecuta en RHEL o CentOS.
Este proceso requiere virsh porque Virt manager no es compatible con el controlador virtio-scsi.

Habilite el cortafuegos VM-Series para usar un controlador SCSI

1. Cree un archivo XML para el controlador SCSI. En este ejemplo, se llama virt-scsi.xml.

```
[root@localhost ~]# cat /root/virt-scsi.xml
<controller type='scsi' index='0' model='virtio-scsi'>
<address type='pci' domain='0x0000' bus='0x00' slot='0x0b'function='0x0'/>
</controller>
```

   Asegúrese de que la ranura usada para el controlador virtio-scsi no crea conflicto con otro dispositivo.

2. Asocie este controlador con la plantilla XML del cortafuegos VM-Series.

```
[root@localhost ~]# virsh attach-device --config <Nombre_VM-Series>
/root/virt-scsi.xml
Device attached successfully
```

3. Habilite el uso del controlador SCSI en el cortafuegos.

```
[root@localhost ~]# virsh attach-disk
<Nombre_VM-Series>/var/lib/libvirt/images/PA-VM-6.1.0-c73.qcow2 sda
--cache none --persistent
Disk attached successfully
```

4. Modifique la plantilla XML en el cortafuegos VM-Series. En la plantilla XML debe cambiar el disco de destino y el bus de disco, usados por el cortafuegos.

   De manera predeterminada, la plantilla XML se almacena en `etc/libvirt/qemu.`

```
<disk type='file' device='disk'>
      <driver name='qemu' type='qcow2' cache='writeback'/>
      <source file='/var/lib/libvirt/images/PA-VM-6.1.0-c73.qcow2'/>
      <target dev='sda' bus='scsi'/>
      <address type='drive' controller='0' bus='0' target='0' unit='0'/>
</disk>
```

Comprobación de PCI-ID para la ordenación de interfaces de red en el cortafuegos VM-Series

Independientemente de que use interfaces virtuales (puente Linux/OVS) o dispositivos PCI (envío PCI o un adaptador compatible con SR-IOV) para la conectividad con el cortafuegos VM-Series, el cortafuegos VM-Series trata la interfaz como un dispositivo PCI. La asignación de una interfaz en el cortafuegos VM-Series se basa en PCI-ID, un valor que combina el bus, dispositivo o ranura y función de la interfaz. Las interfaces se ordenan empezando por el PCI-ID más bajo, lo que significa que la interfaz de gestión (eth0) del cortafuegos se asigna a la interfaz con el PCI-ID más bajo.

Por ejemplo, puede asignar cuatro interfaces al cortafuegos VM-Series: tres interfaces virtuales del tipo virtio y e1000, y la cuarta es un dispositivo PCI. Para ver el PCI-ID de cada interfaz, introduzca el comando `virsh dumpxml $domain <nombre del cortafuegos VM-Series>` en el host Linux para ver la lista de interfaces adjuntadas al cortafuegos VM-Series. En el resultado, compruebe la siguiente configuración de red:

```
<interface type='bridge'>
      <mac address='52:54:00:d7:91:52'/>
      <source bridge='mgmt-br'/>
      <model type='virtio'/>
      <address type='pci' domain='0x0000' bus='0x00' slot='0x03'
function='0x0'/>
    </interface>


 <interface type='bridge'>
      <mac address='52:54:00:f4:62:13'/>
      <source bridge='br8'/>
      <model type='e1000'/>
      <address type='pci' domain='0x0000' bus='0x00' slot='0x10'
function='0x0'/>
    </interface>


  <interface type='bridge'>
      <mac address='52:54:00:fe:8c:80'/>
      <source bridge='br8'/>
      <model type='e1000'/>
      <address type='pci' domain='0x0000' bus='0x00' slot='0x06'
function='0x0'/>
    </interface>
```

```
   <hostdev mode='subsystem' type='pci' managed='yes'>
      <source>
        <address domain='0x0000' bus='0x08' slot='0x10' function='0x1'/>
      </source>
      <address type='pci' domain='0x0000' bus='0x00' slot='0x07'
function='0x0'/>
    </hostdev>
```

En este caso, el PCI-ID de cada interfaz es el siguiente:

- El primer PCI-ID de interfaz virtual es 00:03:00
- El segundo PCI-ID de interfaz virtual es 00:10:00
- El tercer PCI-ID de interfaz virtual es 00:06:00
- El cuarto PCI-ID de interfaz virtual es 00:07:00

Por lo tanto, en el cortafuegos VM-Series, la interfaz con PCI-ID de 00:03:00 se asigna como eth0 (interfaz de gestión), la interfaz con PCI-ID 00:06:00 se asigna como eth1 (ethernet1/1), la interfaz con PCI-ID 00:07:00 es eth2 (ethernet1/2) y la interfaz con PCI-ID 00:10:00 es eth3 (ethernet1/3).

Uso de un archivo ISO para implementar el cortafuegos VM-Series

Si quiere pasar una secuencia de comandos al cortafuegos VM-Series durante el inicio, puede montar un CD-ROM con un archivo ISO. El archivo ISO le permite definir un archivo XML de arranque que incluya los parámetros de configuración inicial para el puerto de gestión del cortafuegos. El cortafuegos VM-Series en el primer inicio comprueba el archivo *bootstrap-networkconfig.xml* y usa los valores definidos en el mismo.

Si se encuentra un solo error en el análisis del archivo de arranque, el cortafuegos VM-Series rechazará toda la configuración en este archivo y se iniciará con los valores predeterminados.

Creación de un archivo ISO de arranque	

Paso 1 Cree el archivo XML y defínalo como una instancia de máquina virtual.
 	
Para un archivo de muestra, consulte Archivo XML de muestra para el cortafuegos VM-Series.
 	
En este ejemplo, el cortafuegos VM-Series se llama PAN_Firewall_DC1.
	Por ejemplo:
	`user-PowerEdge-R510:~/kvm_script$ sudo vi /etc/libvirt/qemu/PAN_Firewall_DC1.xml`
	
	`user-PowerEdge-R510:~/kvm_script$ sudo virsh define/etc/libvirt/qemu/PAN_Firewall_DC1.xml`
	
	`Domain PAN_Firewall_DC1_bootstp defined from /etc/libvirt/qemu/PAN_Firewall_DC1.xml`
	
	`user-PowerEdge-R510:~/kvm_script$ sudo virsh -q attach-interface PAN_Firewall_DC1_bootstp bridge br1 --model=virtio --persistent`
	
	`user-PowerEdge-R510:~/kvm_script$ virsh list --all`
	`Id Name State`
	`----------`
	`- PAN_Firewall_DC1_bootstp shut off`

Paso 2 Cree el archivo XML de arranque.
 	
Puede definir los parámetros de configuración inicial en este archivo y dele el nombre *bootstrap-networkconfig*.
 	
Si no quiere incluir un parámetro, por ejemplo, panorama-server-secondary. Elimine la línea entera del archivo. Si deja el campo de dirección IP vacío, el archivo no se analizará correctamente.
	Use el siguiente ejemplo como plantilla para el archivo bootstrap-networkconfig. El archivo bootstrap-networkconfig puede incluir solamente los siguientes parámetros:
	`<vm-initcfg>`
	`<hostname>VM_ABC_Company</hostname>`
	`<ip-address>10.5.132.162</ip-address>`
	`<netmask>255.255.254.0</netmask>`
	`<default-gateway>10.5.132.1</default-gateway>`
	`<dns-primary>10.44.2.10</dns-primary>`
	`<dns-secondary>8.8.8.8</dns-secondary>`
	`<panorama-server-primary>10.5.133.4</panorama-server-primary>`
	`<panorama-server-secondary>10.5.133.5</panorama-server-secondary>`
	`</vm-initcfg>`

Paso 3 Cree el archivo ISO. En este ejemplo, usamos mkisofs. Guarde el archivo ISO en el directorio de imágenes (/var/lib/libvirt/image) o el directorio qemu (/etc/libvirt/qemu) para asegurarse de que el cortafuegos tiene acceso de lectura al archivo ISO.	Por ejemplo: `# mkisofs -J -R -v -V "Bootstrap" -A "Bootstrap" -ldots -l -allow-lowercase -allow-multidot -o <iso-filename> bootstrap-networkconfig.xml`
Paso 4 Adjunte el archivo ISO en el CD-ROM.	Por ejemplo: `# virsh -q attach-disk <vm-name> <iso-filename> sdc --type cdrom --mode readonly -persistent\`

Archivo XML de muestra para el cortafuegos VM-Series

```
<?xml version="1.0"?>
<domain type="kvm">
    <name>PAN_Firewall_DC1</name>
    <memory>4194304</memory>
    <currentMemory>4194304</currentMemory>
    <vcpu placement="static">2</vcpu>
    <os>
      <type arch="x86_64">hvm</type>
      <boot dev="hd"/>
    </os>
    <features>
      <acpi/>
      <apic/>
      <pae/>
    </features>
    <clock offset="utc"/>
    <on_poweroff>destroy</on_poweroff>
    <on_reboot>restart</on_reboot>
    <on_crash>restart</on_crash>
    <devices>
      <emulator>/usr/libexec/qemu-kvm</emulator>
      <disk type="file" device="disk">
          <driver type="qcow2" name="qemu"/>
          <source file="/var/lib/libvirt/images/panos-kvm.qcow2"/>
          <target dev="vda" bus="virtio"/>
          </disk>
      <controller type="usb" index="0"/>
      <controller type="ide" index="0"/>
      <controller type="scsi" index="0"/>
      <serial type="pty">
          <source path="/dev/pts/1"/>
          <target port="0"/>
          <alias name="serial0"/>
          </serial>
      <console type="pty" tty="/dev/pts/1">
          <source path="/dev/pts/1"/>
          <target type="serial" port="0"/>
          <alias name="serial0"/>
```

```
        </console>
    <input type="mouse" bus="ps2"/>
    <graphics type="vnc" port="5900" autoport="yes"/>
  </devices>
</domain>
```